Figure 1

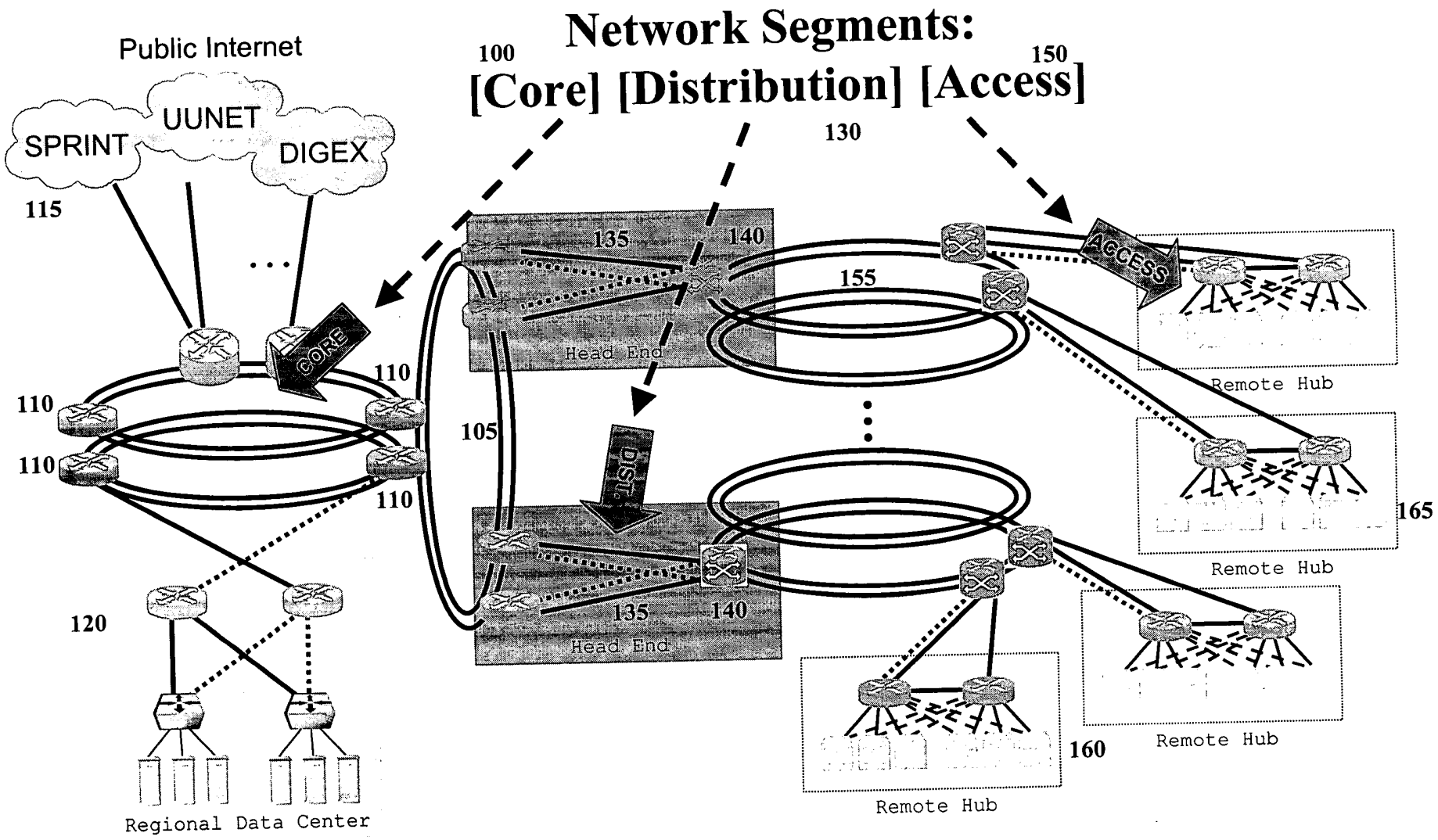

Network Segments:
[Core] [Distribution] [Access]
100
150
130
Public Internet
SPRINT
UUNET
DIGEX
115
CORE
DIST
ACCESS
135
140
155
Head End
110
105
120
165
160
Remote Hub
Regional Data Center

Figure 2

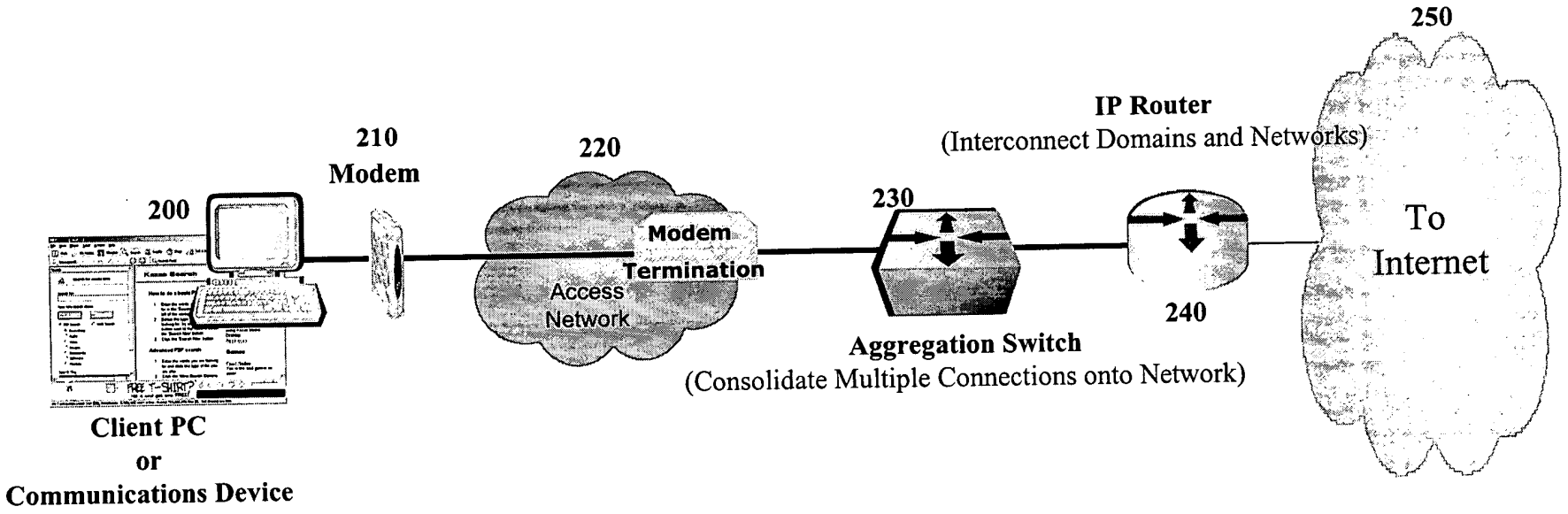

250
IP Router
(Interconnect Domains and Networks)
210
Modem
220
200
230
Modem
Termination
Access
Network
To
Internet
240
Aggregation Switch
(Consolidate Multiple Connections onto Network)
Client PC
or
Communications Device

Figure 3

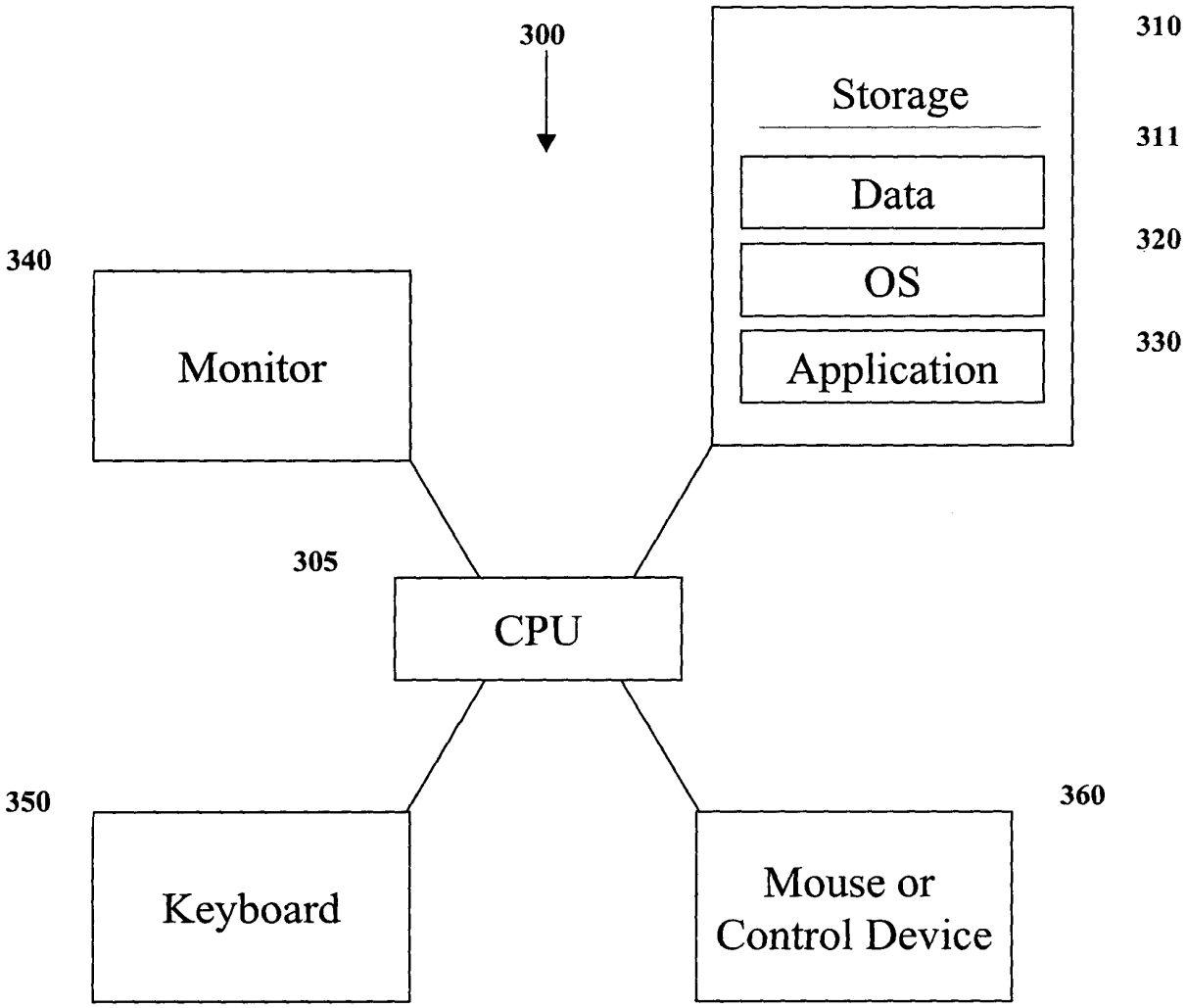

300
310
Storage
311
Data
320
OS
330
Application
340
Monitor
305
CPU
350
Keyboard
360
Mouse or
Control Device

Figure 4

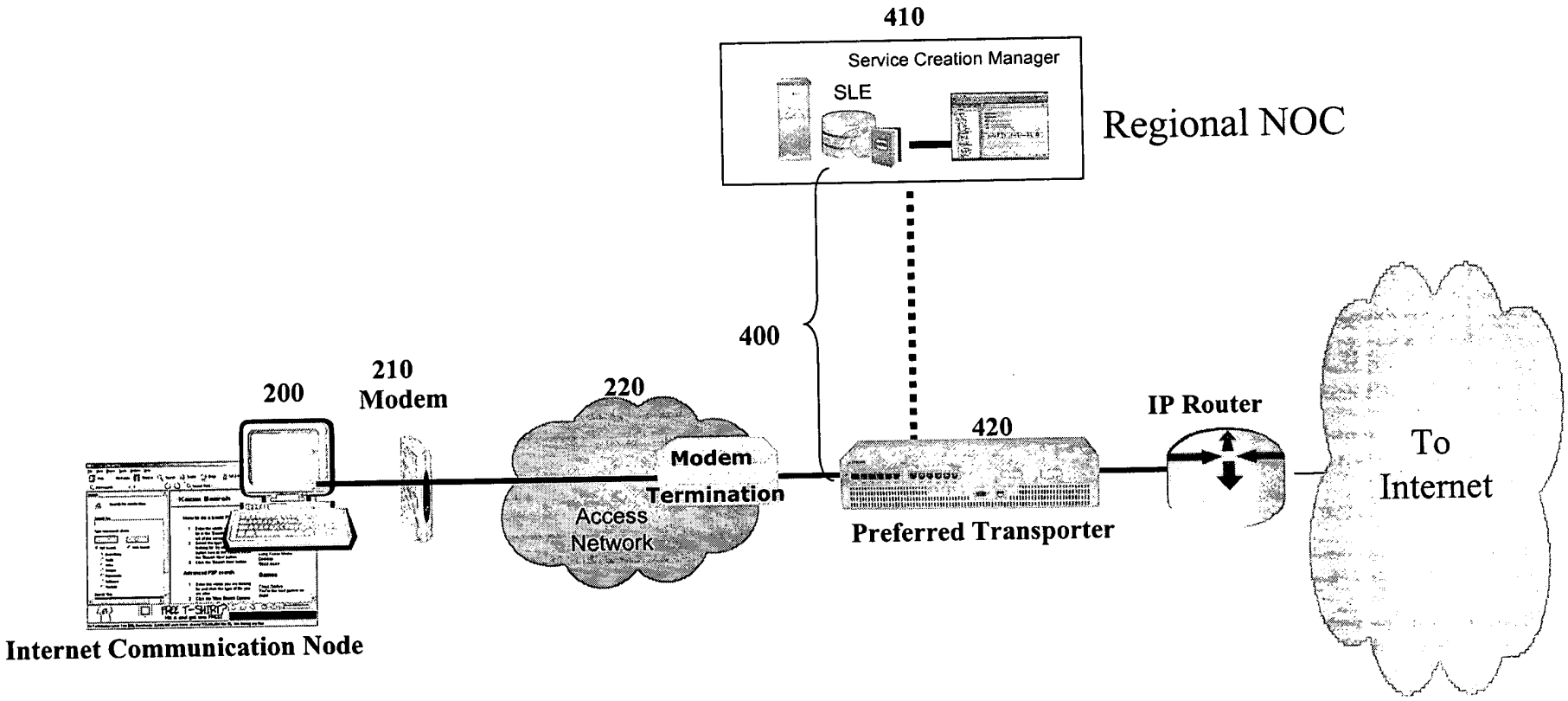

410
Service Creation Manager
SLE
Regional NOC
400
200
210
Modem
220
Modem
Termination
Access
Network
420
IP Router
Preferred Transporter
To
Internet
Internet Communication Node

Figure 5

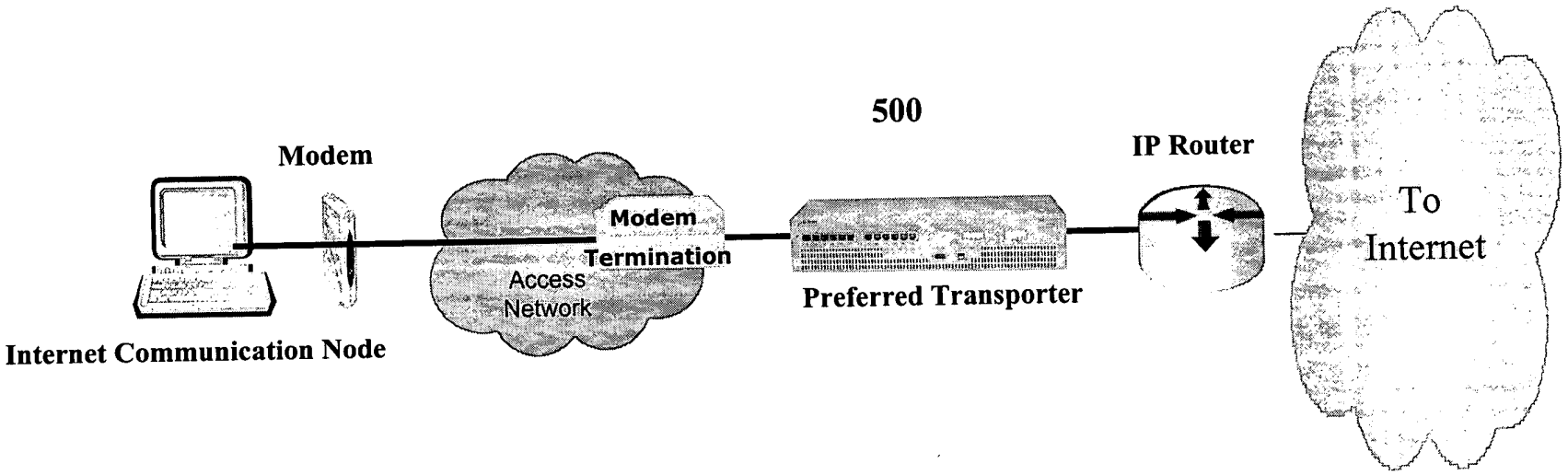
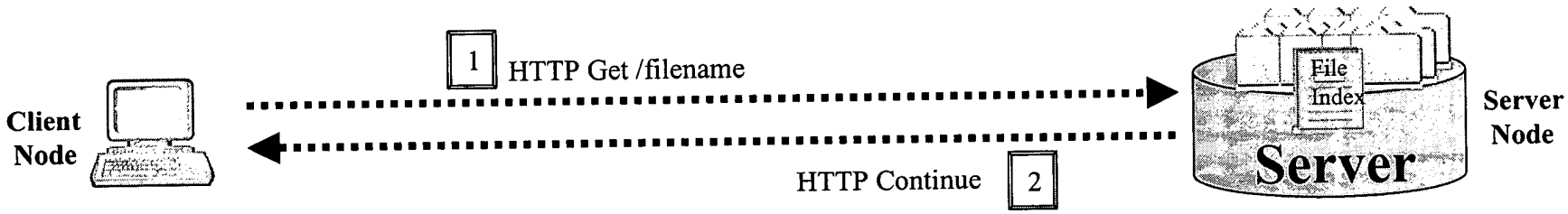

500
Modem
IP Router
Modem
Termination
Access
Network
To
Internet
Internet Communication Node
Preferred Transporter

Figure 6

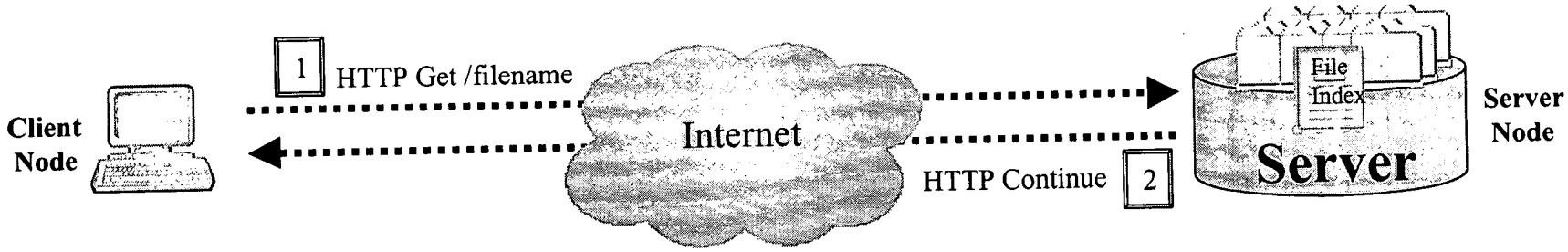
In Client/Server networks, nodes act only as clients



1. Client requests file
2. Server returns file

Figure 7

In Client/Server networks, nodes act only as clients



1. Client requests file
2. Server returns file

Figure 8

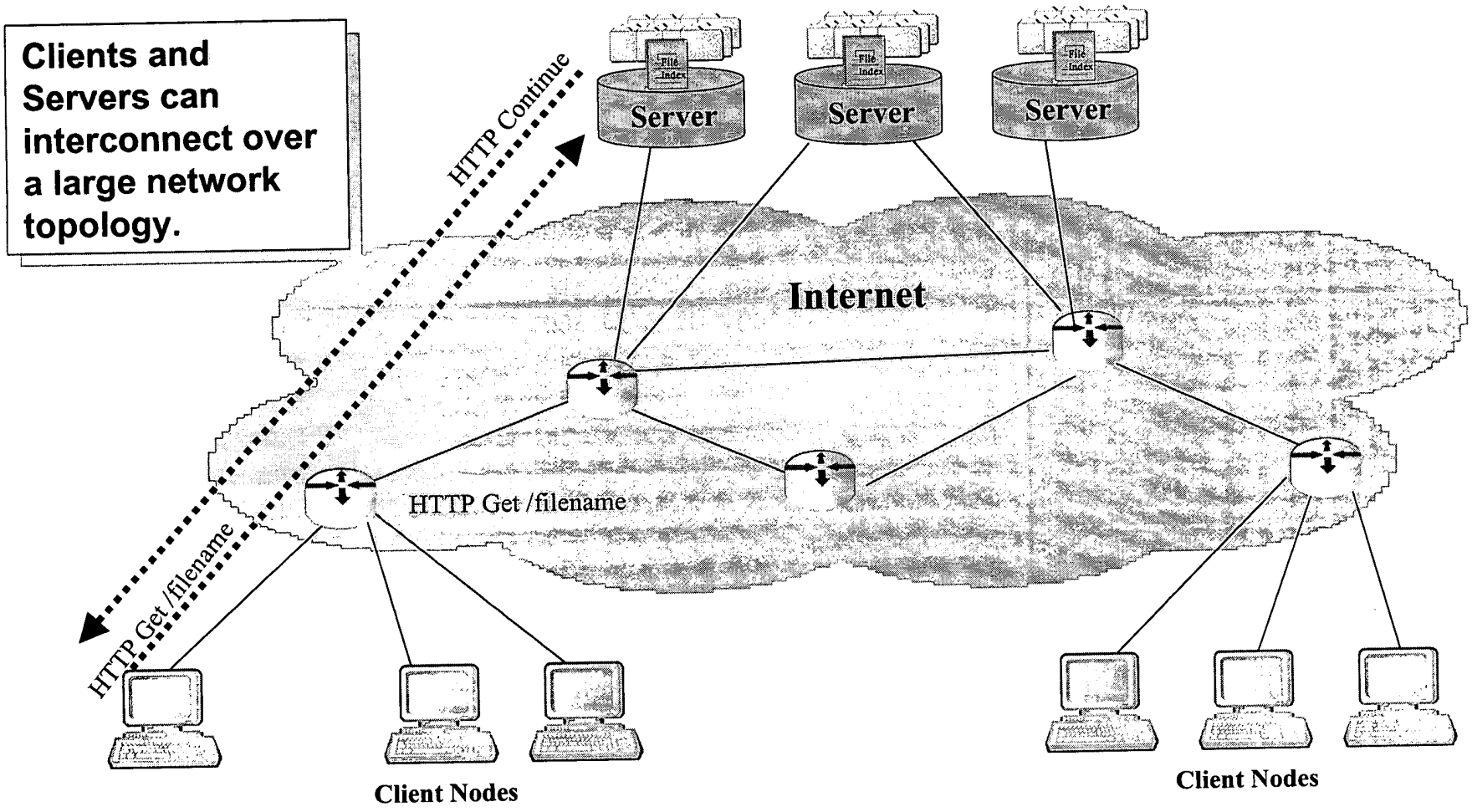
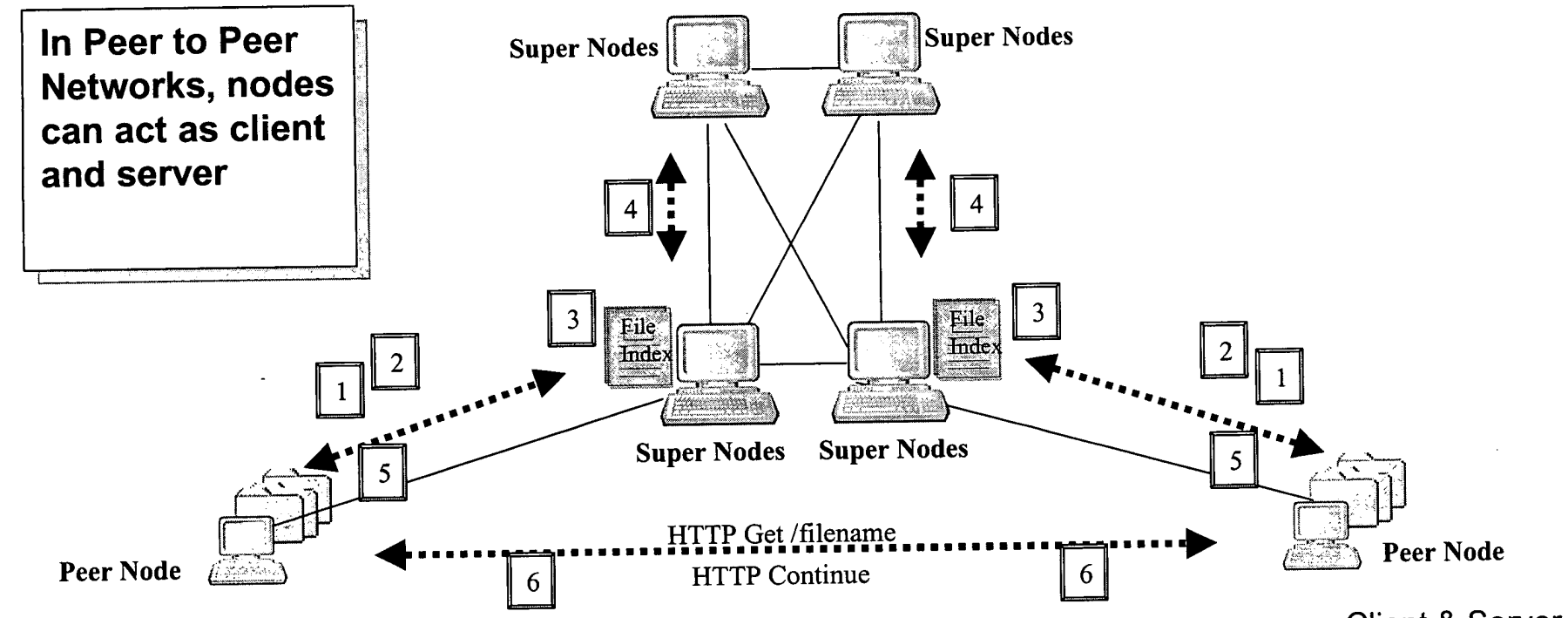

Clients and Servers can interconnect over a large network topology.
HTTP Continue
HTTP Get /filename
Server
Server
Server
Internet
HTTP Get /filename
Client Nodes
Client Nodes

Figure 9



1. Peer Node finds Super Node
2. Peer Node registers files to share with Super Node
3. Super Node maintains index of shared files and Peer Nodes
4. Super Nodes search other Super Nodes
5. Super Node returns Peer Node that has copy of requested file
6. Peer Nodes then communicate directly to transfer file

Figure 10

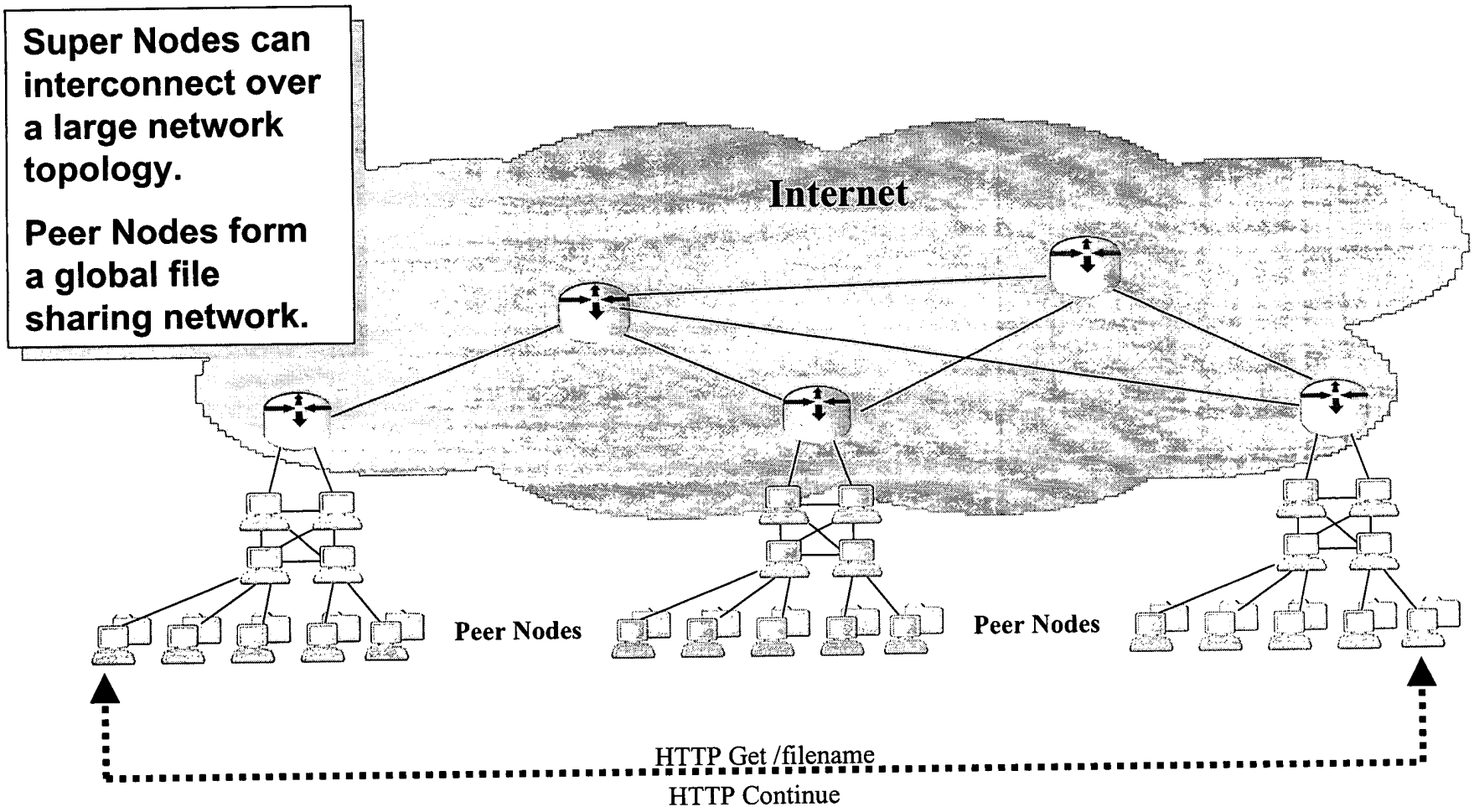

Super Nodes can interconnect over a large network topology.
Peer Nodes form a global file sharing network.
Internet
Peer Nodes
Peer Nodes
HTTP Get /filename
HTTP Continue

Figure 11

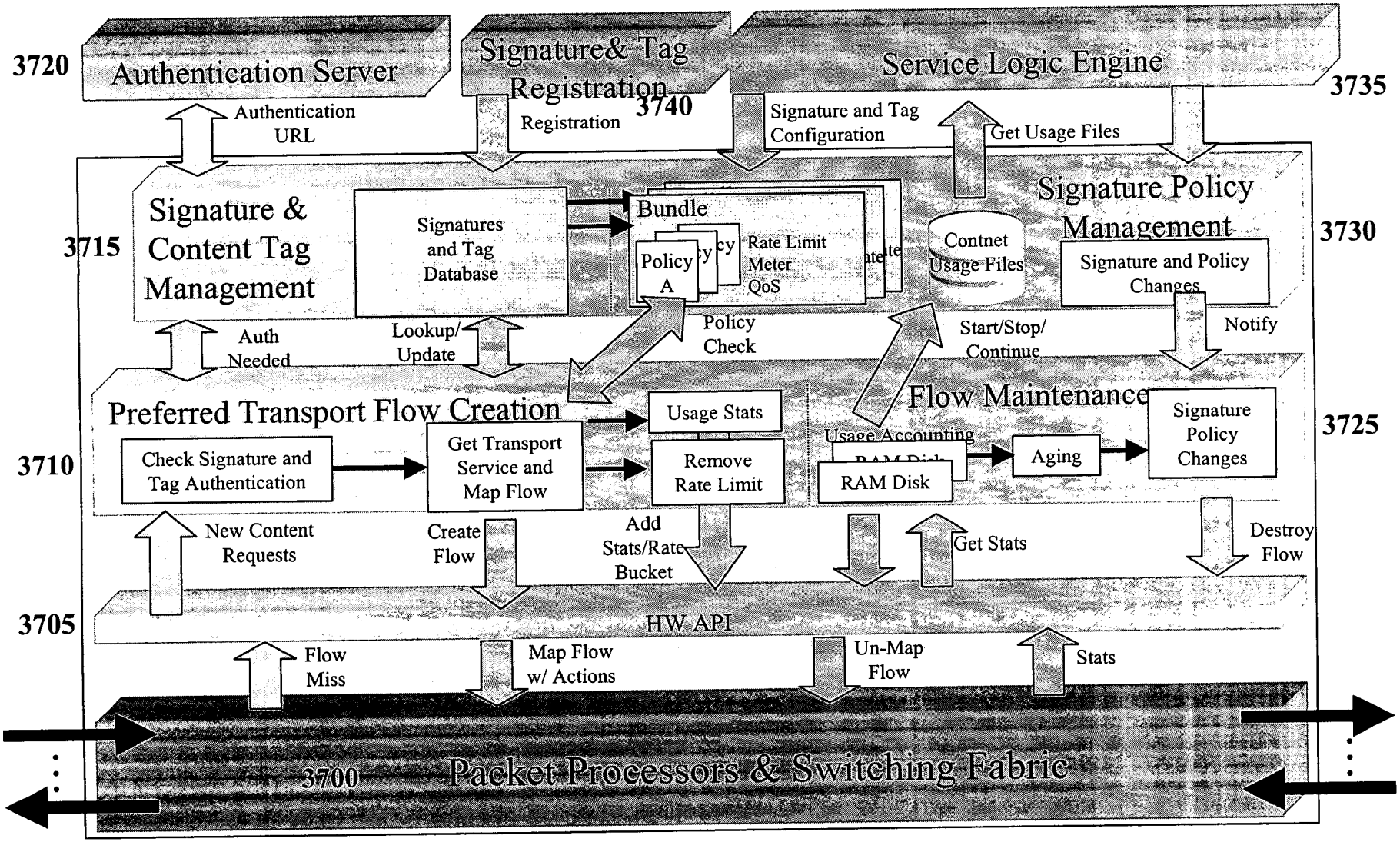

3720
Authentication Server
Signature& Tag Registration
3740
Service Logic Engine
3735
Authentication URL
Registration
Signature and Tag Configuration
Get Usage Files
3715
Signature & Content Tag Management
Signatures and Tag Database
Bundle
Policy A
Rate Limit Meter QoS
Contnet Usage Files
Signature Policy Management
3730
Signature and Policy Changes
Auth Needed
Lookup/ Update
Policy Check
Start/Stop/ Continue
Notify
Preferred Transport Flow Creation
Usage Stats
Flow Maintenance
3725
3710
Check Signature and Tag Authentication
Get Transport Service and Map Flow
Remove Rate Limit
Usage Accounting
RAM Disk
Aging
Signature Policy Changes
New Content Requests
Create Flow
Add Stats/Rate Bucket
Get Stats
Destroy Flow
3705
HW API
Flow Miss
Map Flow w/ Actions
Un-Map Flow
Stats
3700
Packet Processors & Switching Fabric

Figure 12

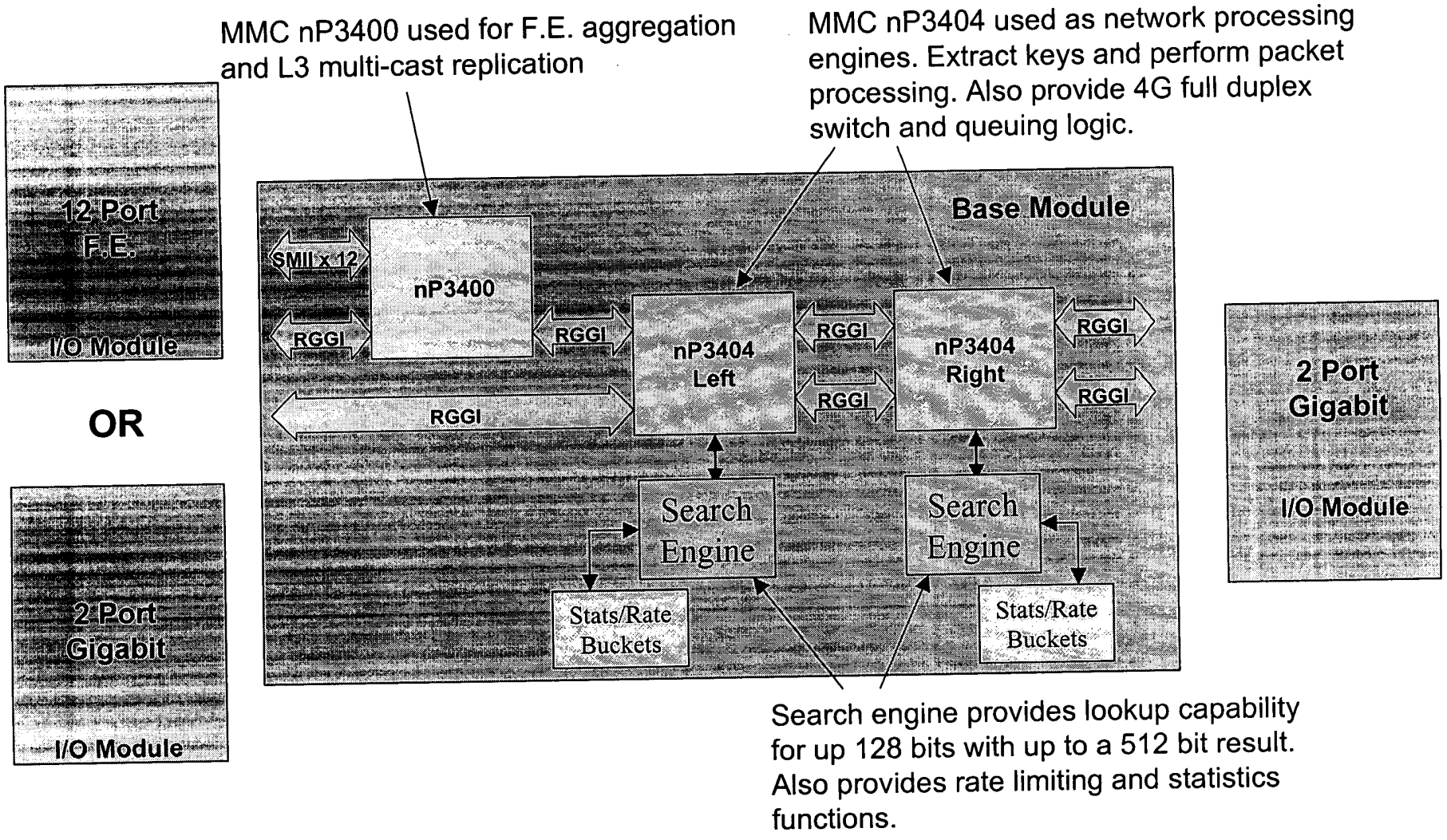

MMC nP3400 used for F.E. aggregation and L3 multi-cast replication
MMC nP3404 used as network processing engines. Extract keys and perform packet processing. Also provide 4G full duplex switch and queuing logic.
12 Port F.E. I/O Module
OR
2 Port Gigabit I/O Module
Base Module
SMII x 12
nP3400
RGGI
nP3404 Left
nP3404 Right
Search Engine
Search Engine
Stats/Rate Buckets
Stats/Rate Buckets
2 Port Gigabit I/O Module
Search engine provides lookup capability for up 128 bits with up to a 512 bit result. Also provides rate limiting and statistics functions.

Figure 13

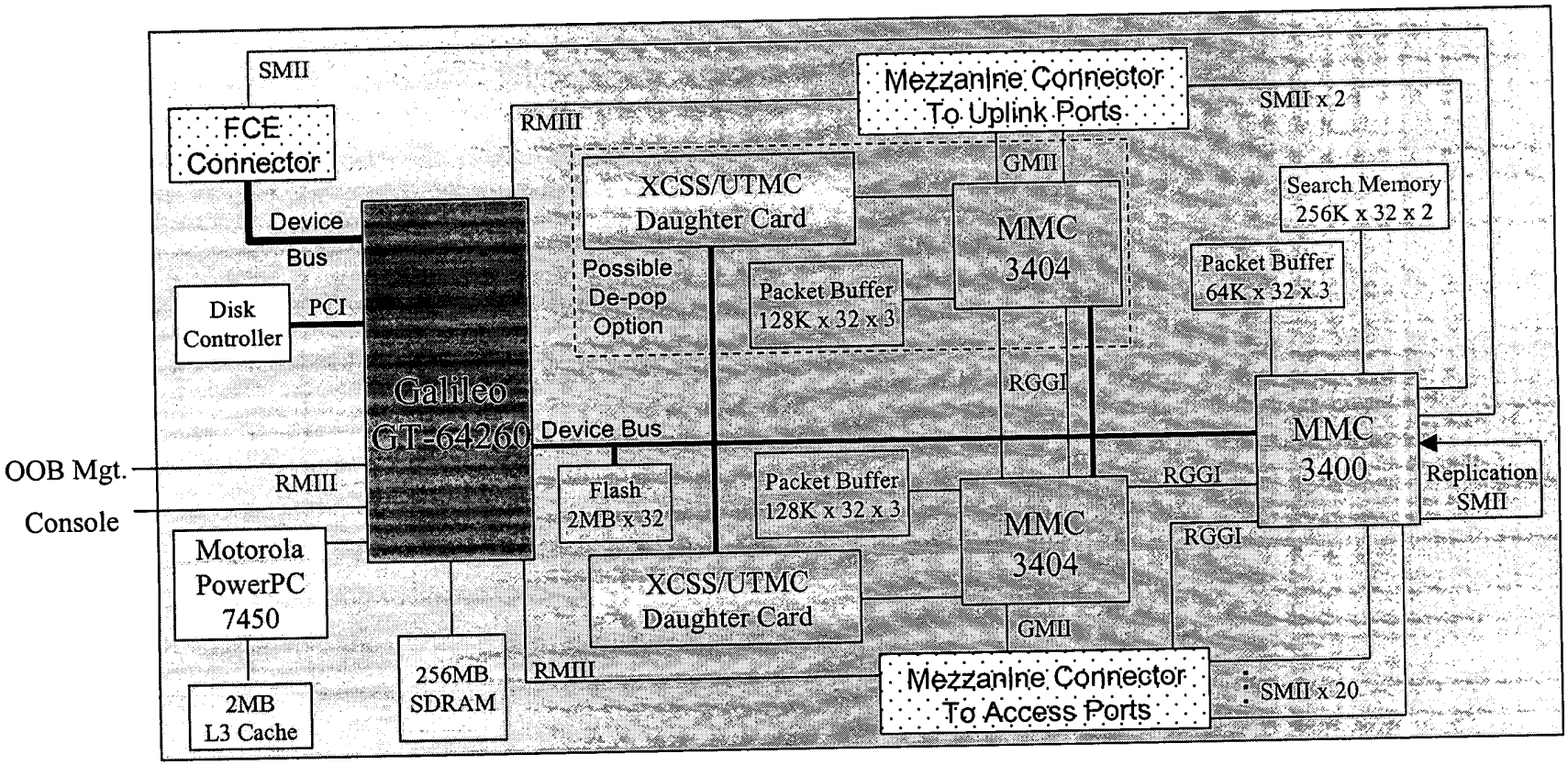

SMII
FCE Connector
Device Bus
Disk Controller
PCI
Galileo GT-64260
OOB Mgt.
RMIII
Console
Motorola PowerPC 7450
2MB L3 Cache
256MB SDRAM
RMIII
Mezzanine Connector To Uplink Ports
SMII x 2
GMII
XCSS/UTMC Daughter Card
Possible De-pop Option
Packet Buffer 128K x 32 x 3
MMC 3404
Search Memory 256K x 32 x 2
Packet Buffer 64K x 32 x 3
RGGI
Device Bus
Flash 2MB x 32
Packet Buffer 128K x 32 x 3
MMC 3404
RGGI
MMC 3400
Replication SMII
RGGI
XCSS/UTMC Daughter Card
GMII
RMIII
Mezzanine Connector To Access Ports
SMII x 20

Figure 14

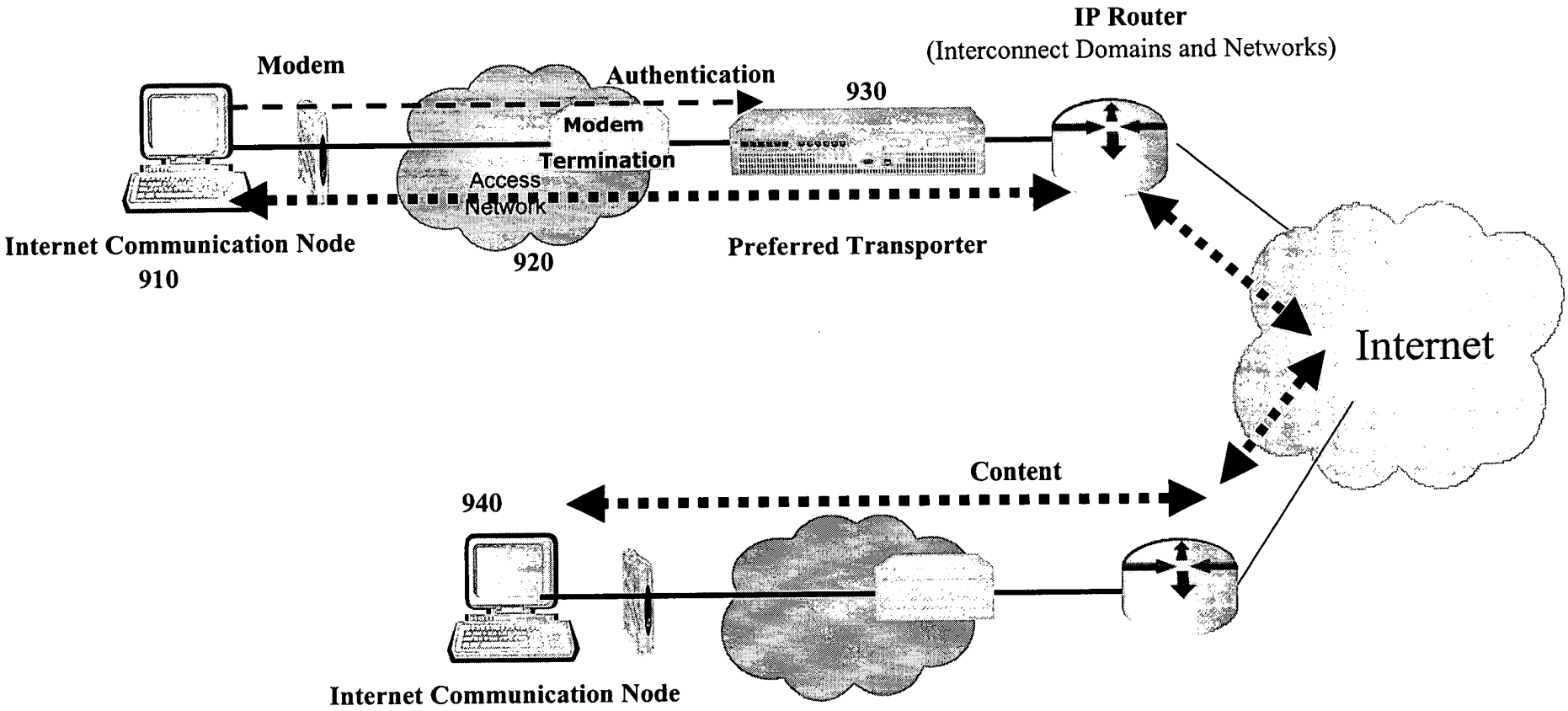

IP Router
(Interconnect Domains and Networks)
Modem
Authentication
930
Modem
Termination
Access
Network
Internet Communication Node
910
920
Preferred Transporter
Internet
Content
940
Internet Communication Node

Figure 15

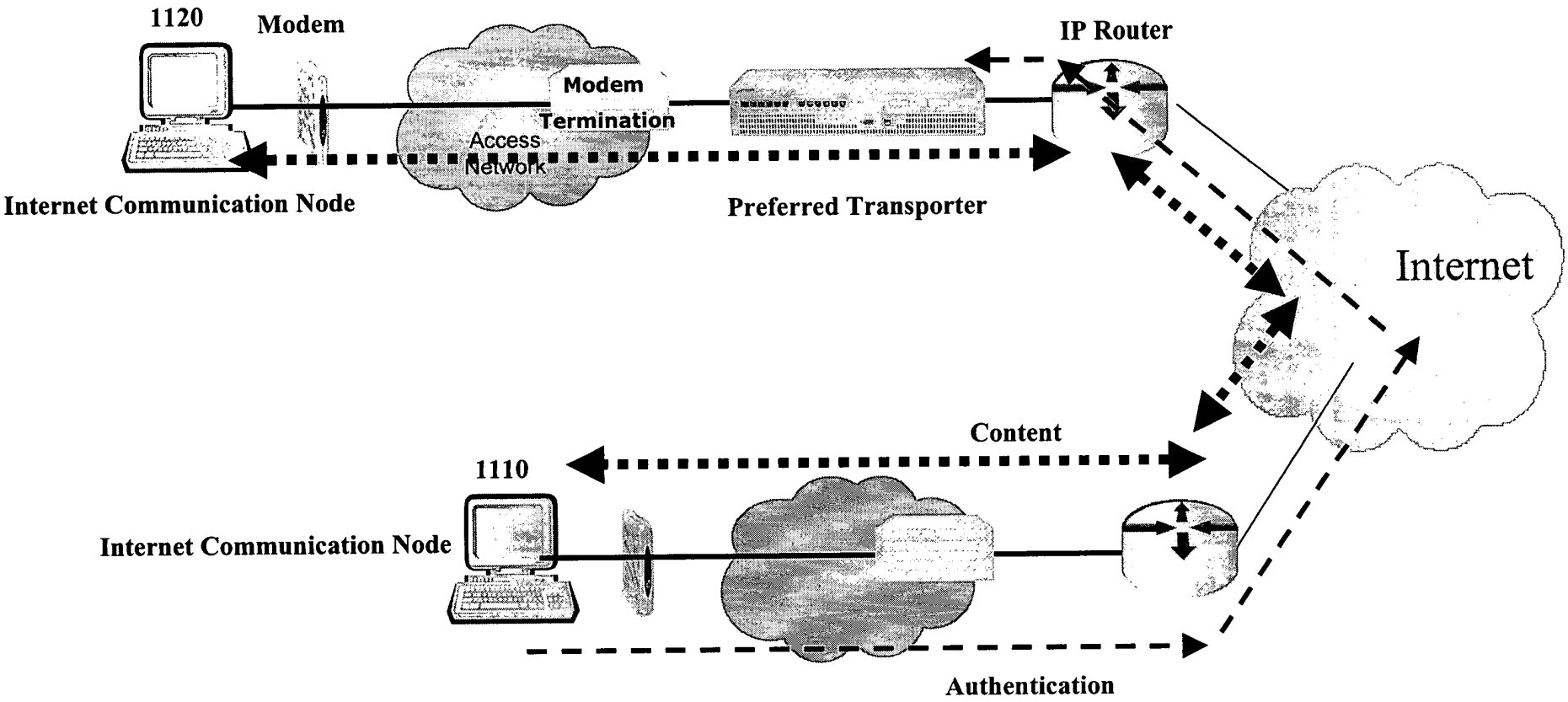

1120
Modem
Modem
Termination
Access
Network
IP Router
Internet Communication Node
Preferred Transporter
Internet
Content
1110
Internet Communication Node
Authentication

Figure 16

METHOD AND SYSTEM FOR TAGGING CONTENT
FOR PREFERRED TRANSPORT
DOCKET NO: 026215-00003
Kurt A. DOBBINS et al.

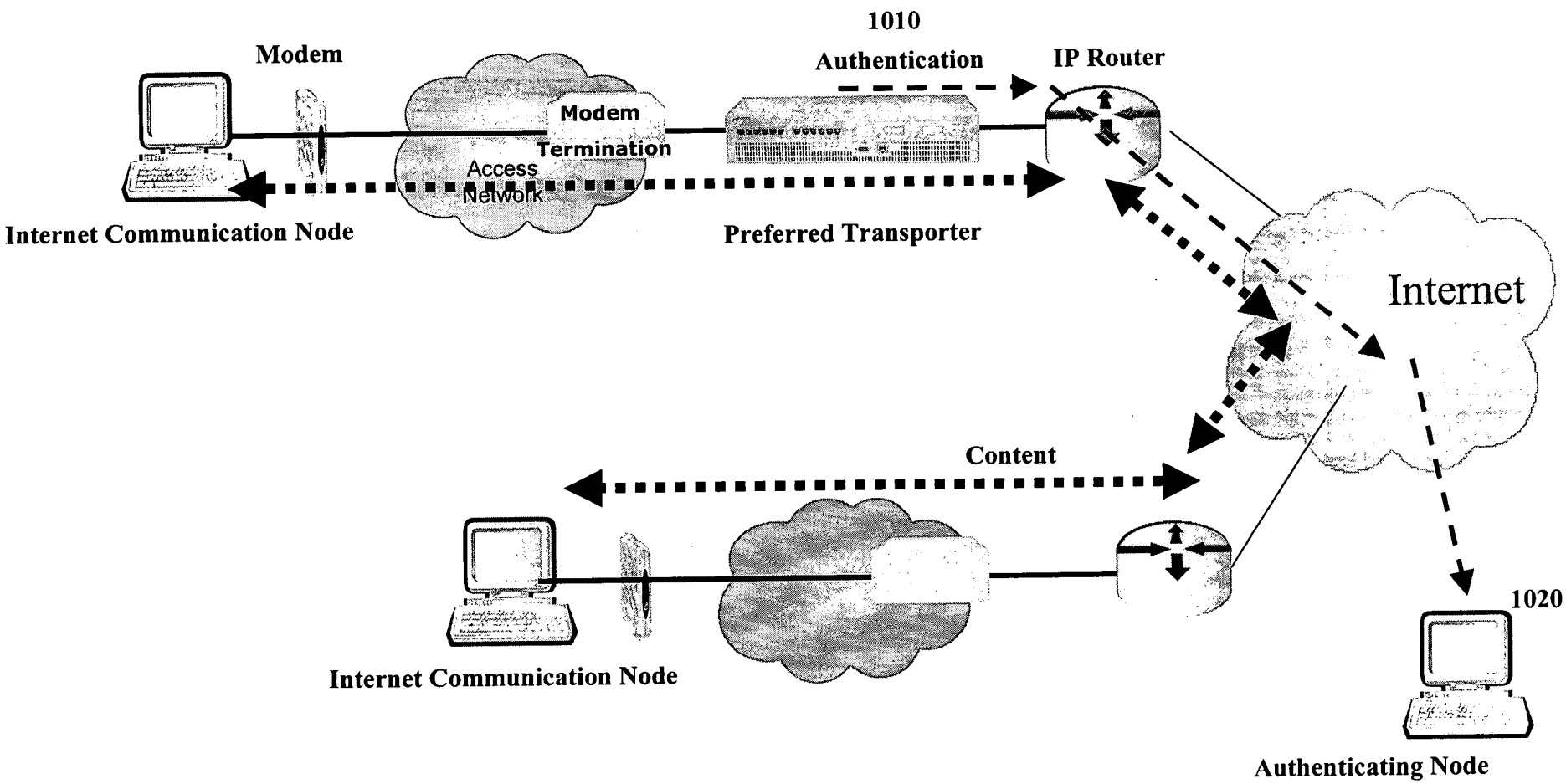


Figure 17

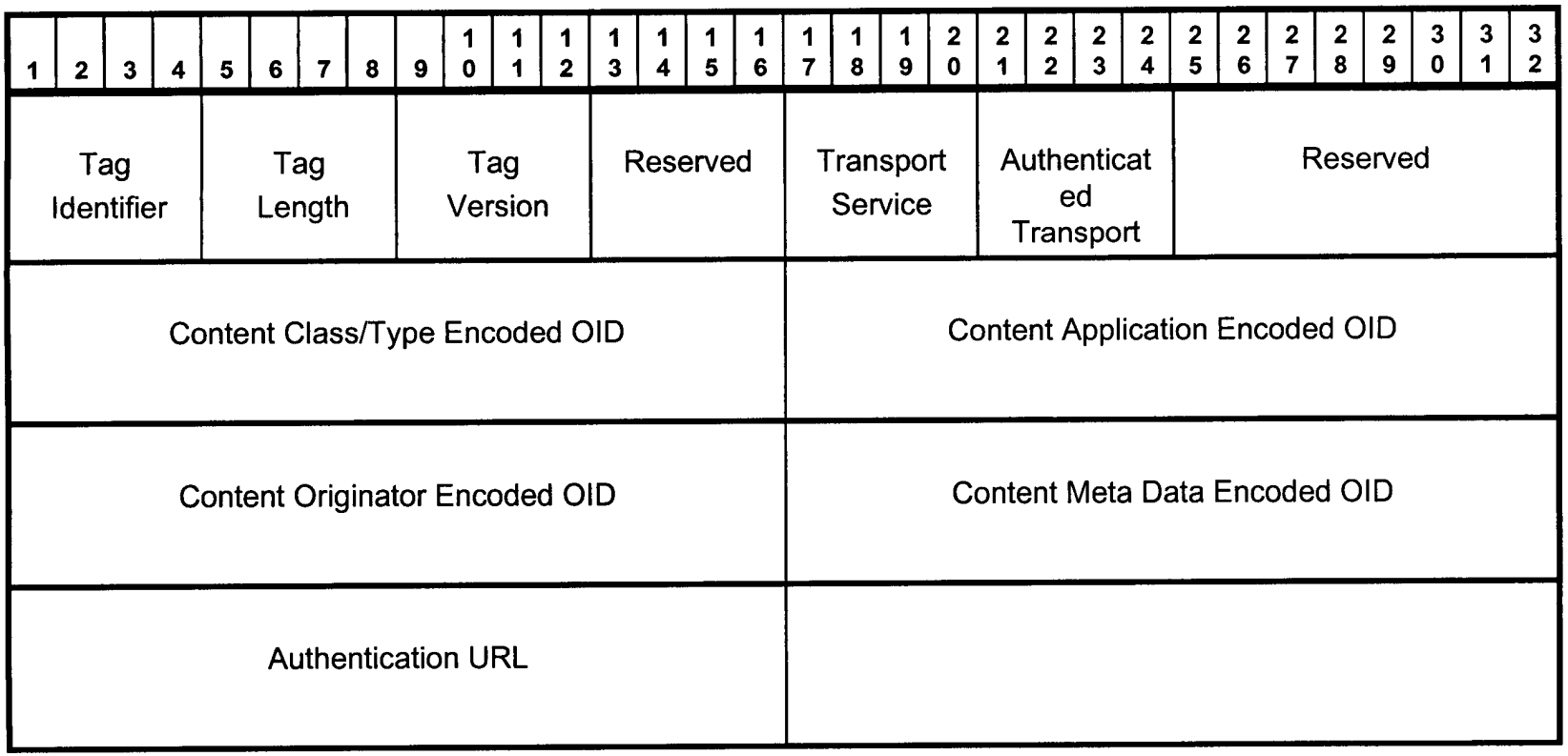

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
Tag Identifier
Tag Length
Tag Version
Reserved
Transport Service
Authenticated Transport
Reserved
Content Class/Type Encoded OID
Content Application Encoded OID
Content Originator Encoded OID
Content Meta Data Encoded OID
Authentication URL

Figure 18

Field	Length (bytes)	Description	Comments
Tag ID	4	Well-known tag identifier. Allows different tag types to be supported	Value set to "AUTH"
Tag Length	4	Indicates the remaining length of the tag.	Maximum Length of 128 bytes
Tag Version	4	Version of Tag Structure	Value set to "1.0"
Reserved	4	Reserved for Future Use	Unused
Transport Service	4	Preferred Transport Bit Mask for Transport Service Preference.	1 = No Rate Limit 2 = No Byte Cap 4 = On-Demand BW 8 = BLOCK ACCESS
Authenticated Transport	4	Digital Signature used to authenticate preferred transport	
Reserved	8	Reserved for Future Use	Unused
Content Class/Type	16	OID syntax from Content Class naming tree.	Encoded using ASN.1 BER {tag/len/value}
Content Application	16	OID syntax from Application naming tree.	Encoded using ASN.1 BER {tag/len/value}
Content Originator	16	OID syntax from Content Originator naming tree.	Encoded using ASN.1 BER {tag/len/value}
Content Meta Data	16	OID syntax from Content Meta Data naming tree.	Encoded using ASN.1 BER {tag/len/value}
Authentication URL	32	URL of authentication server	

Figure 19

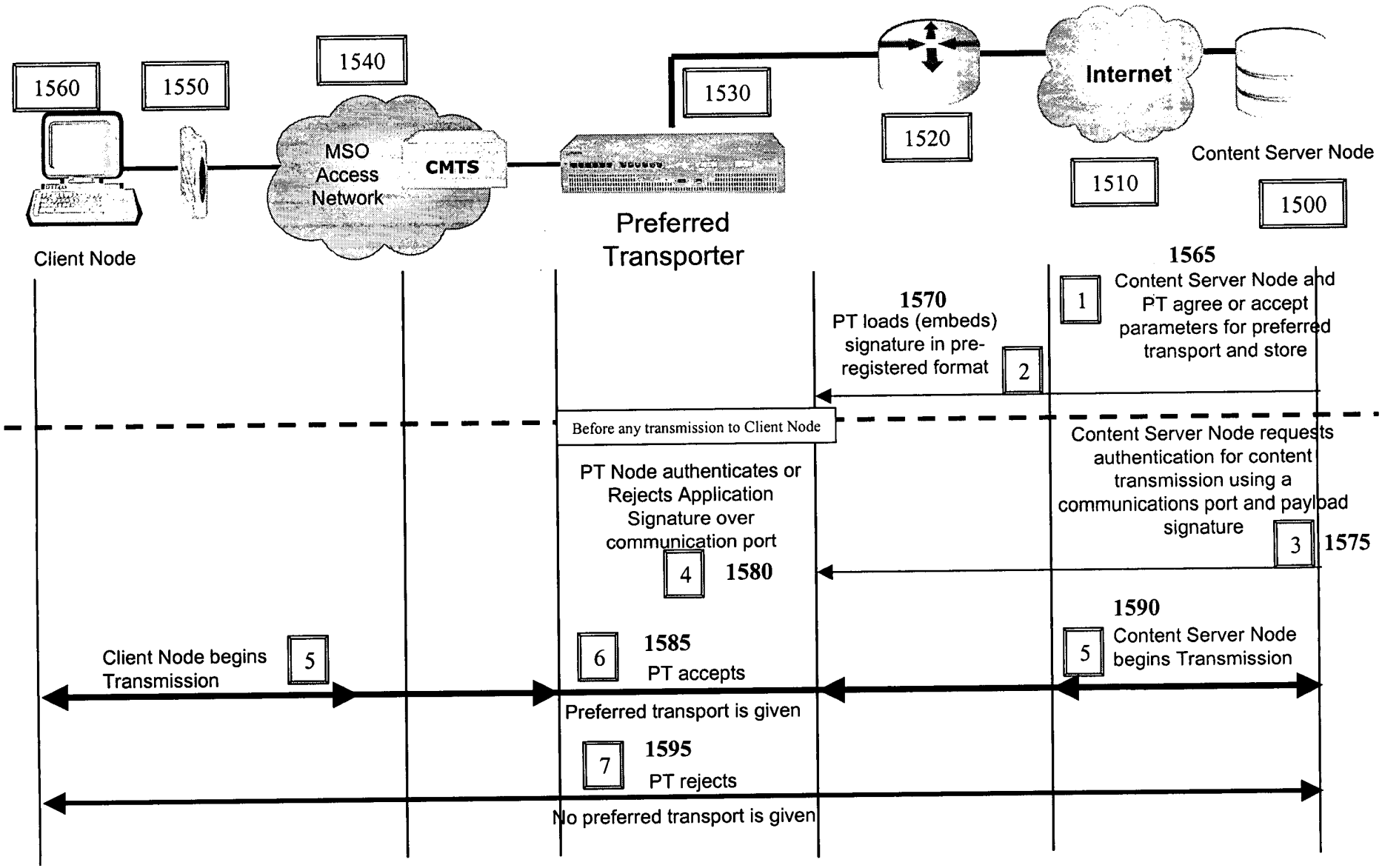

1560
1550
1540
1530
1520
Internet
1510
Content Server Node
1500
MSO
Access
Network
CMTS
Client Node
Preferred
Transporter
1565
1
Content Server Node and
PT agree or accept
parameters for preferred
transport and store
1570
PT loads (embeds)
signature in pre-
registered format
2
Before any transmission to Client Node
Content Server Node requests
authentication for content
transmission using a
communications port and payload
signature
3
1575
PT Node authenticates or
Rejects Application
Signature over
communication port
4
1580
1590
Client Node begins
Transmission
5
6
1585
PT accepts
5
Content Server Node
begins Transmission
Preferred transport is given
7
1595
PT rejects
No preferred transport is given

Figure 19a

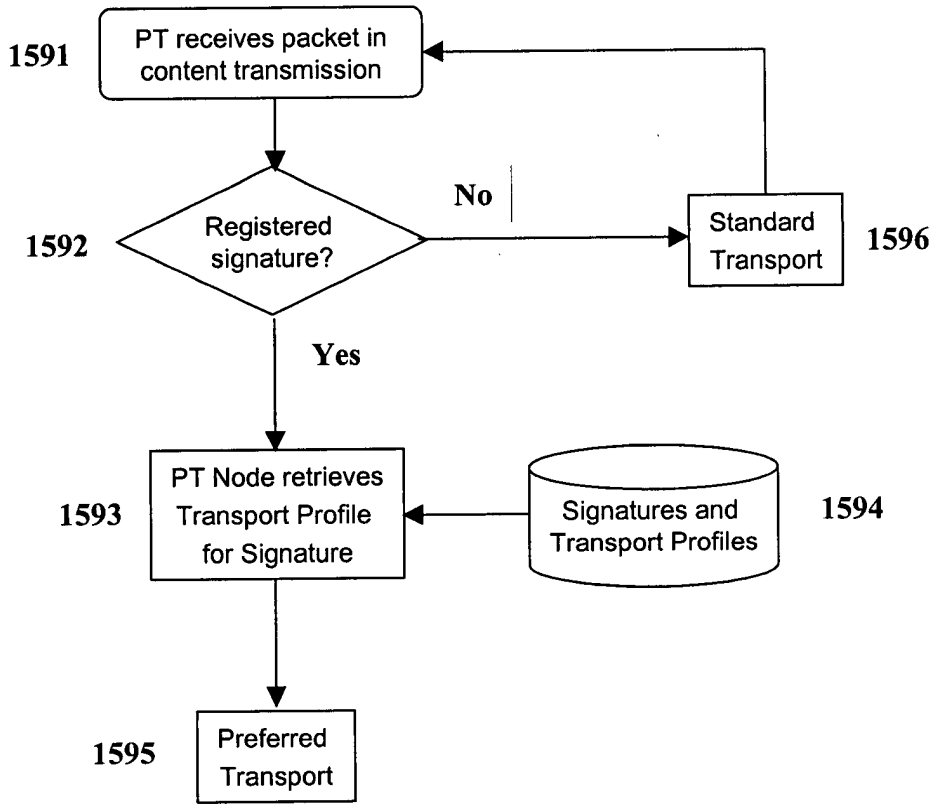

1591
PT receives packet in content transmission
1592
Registered signature?
No
Standard Transport
1596
Yes
1593
PT Node retrieves Transport Profile for Signature
Signatures and Transport Profiles
1594
1595
Preferred Transport

Figure 20

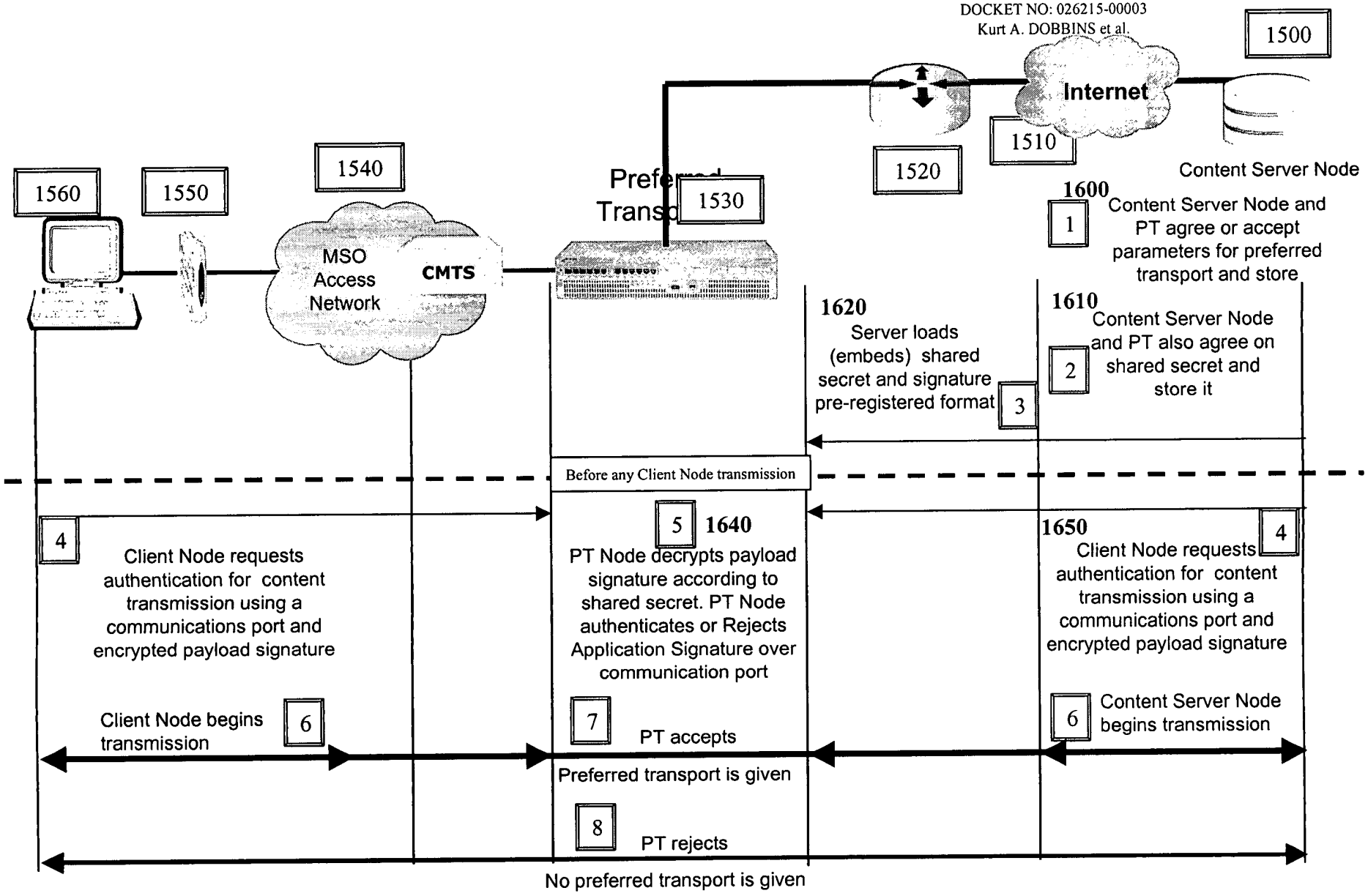

1500
Internet
1510
1520
Content Server Node
1600
1
Content Server Node and PT agree or accept parameters for preferred transport and store
1560
1550
1540
MSO Access Network
CMTS
1530
1620
Server loads (embeds) shared secret and signature pre-registered format
3
1610
2
Content Server Node and PT also agree on shared secret and store it
Before any Client Node transmission
4
Client Node requests authentication for content transmission using a communications port and encrypted payload signature
5
1640
PT Node decrypts payload signature according to shared secret. PT Node authenticates or Rejects Application Signature over communication port
1650
4
Client Node requests authentication for content transmission using a communications port and encrypted payload signature
Client Node begins transmission
6
7
PT accepts
6
Content Server Node begins transmission
Preferred transport is given
8
PT rejects
No preferred transport is given

Figure 20a

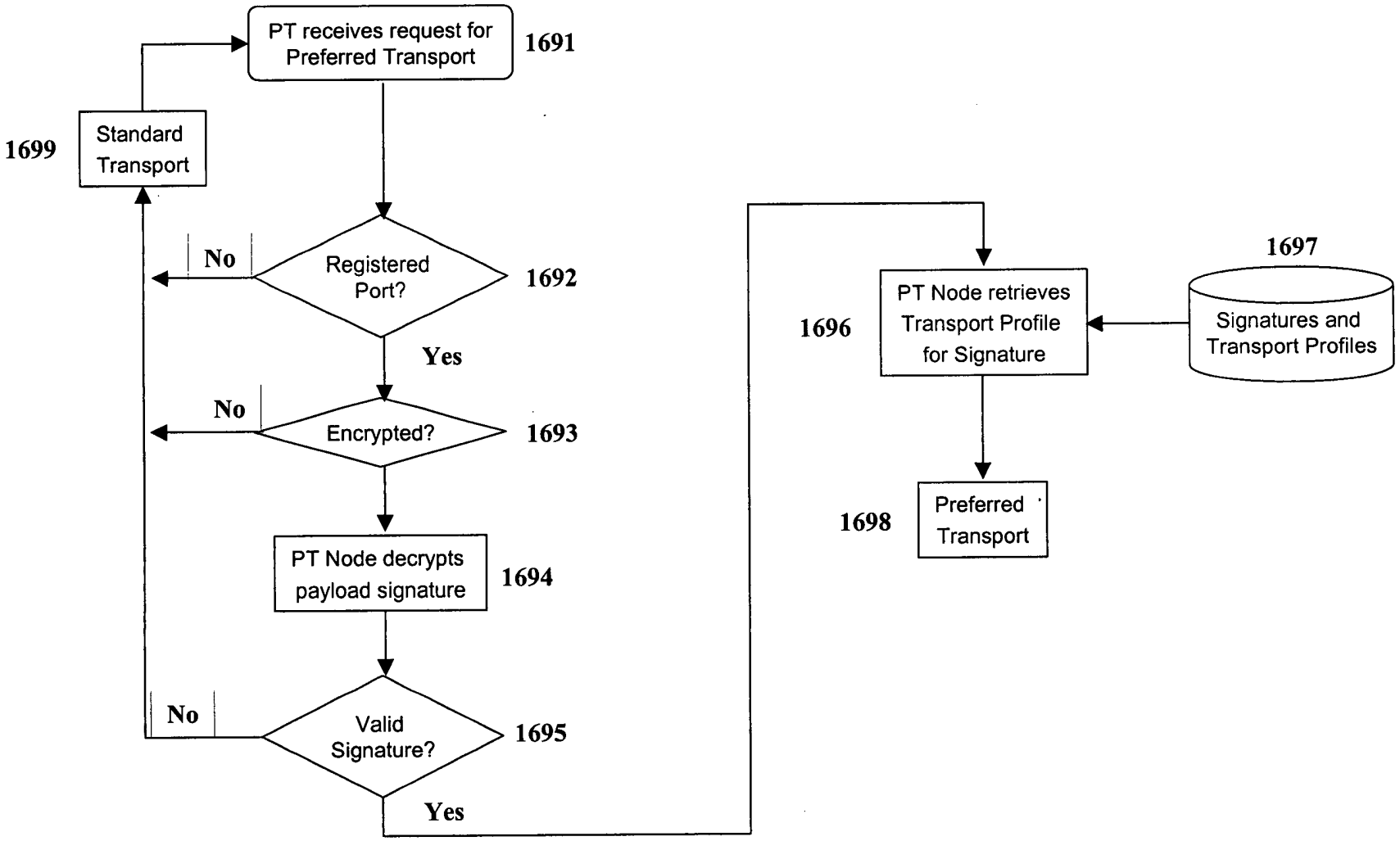

PT receives request for Preferred Transport
1691
1699
Standard Transport
No
Registered Port?
1692
Yes
No
Encrypted?
1693
PT Node decrypts payload signature
1694
No
Valid Signature?
1695
Yes
1697
PT Node retrieves Transport Profile for Signature
1696
Signatures and Transport Profiles
1698
Preferred Transport

Fig 21

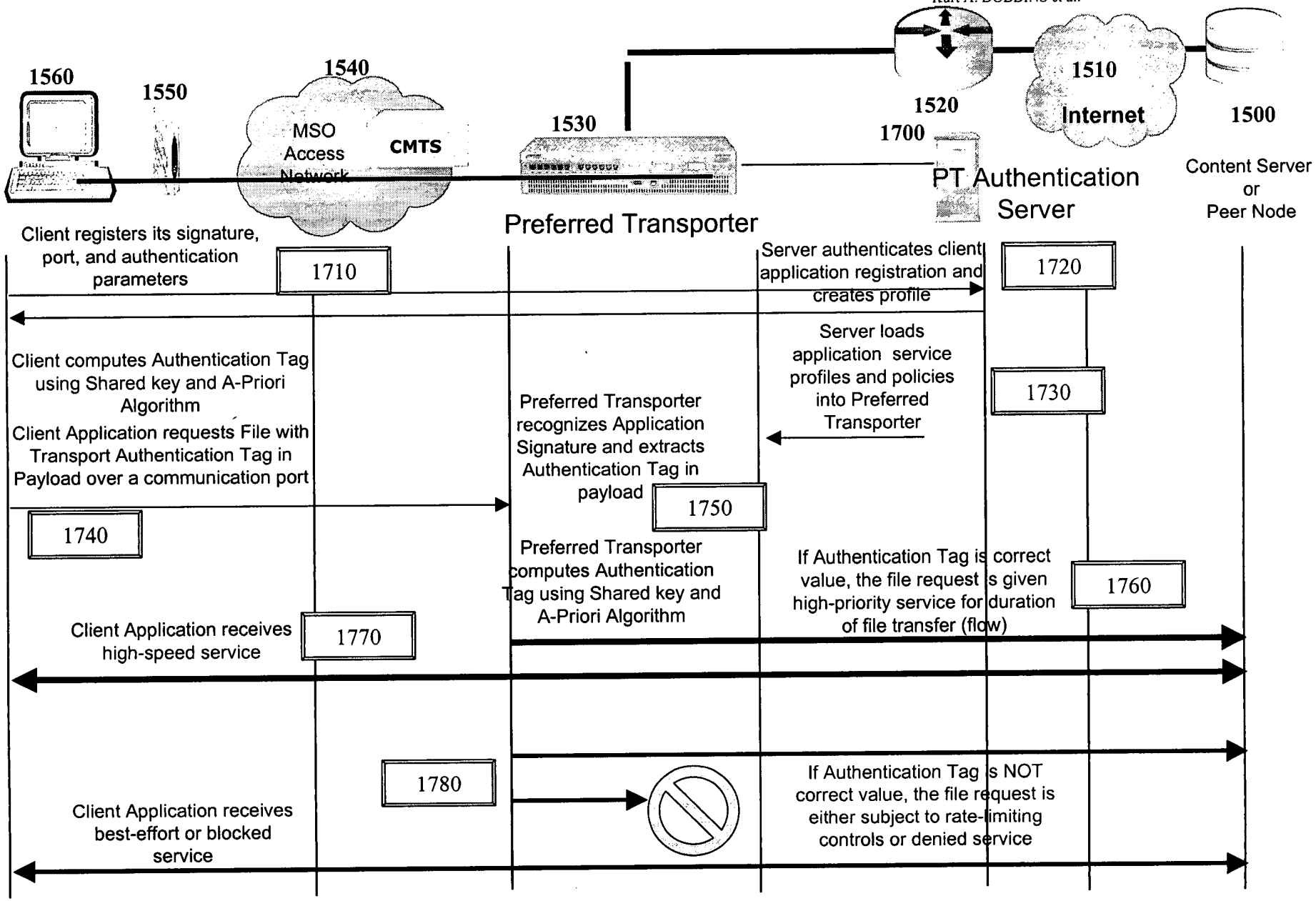

1560
1550
1540
MSO
Access
Network
CMTS
1530
1520
1700
1510
Internet
1500
PT Authentication
Server
Content Server
or
Peer Node
Preferred Transporter
Client registers its signature, port, and authentication parameters
1710
Server authenticates client application registration and creates profile
1720
Server loads application service profiles and policies into Preferred Transporter
1730
Client computes Authentication Tag using Shared key and A-Priori Algorithm
Client Application requests File with Transport Authentication Tag in Payload over a communication port
1740
Preferred Transporter recognizes Application Signature and extracts Authentication Tag in payload
1750
Preferred Transporter computes Authentication Tag using Shared key and A-Priori Algorithm
If Authentication Tag is correct value, the file request is given high-priority service for duration of file transfer (flow)
1760
Client Application receives high-speed service
1770
1780
Client Application receives best-effort or blocked service
If Authentication Tag is NOT correct value, the file request is either subject to rate-limiting controls or denied service

Figure 21a

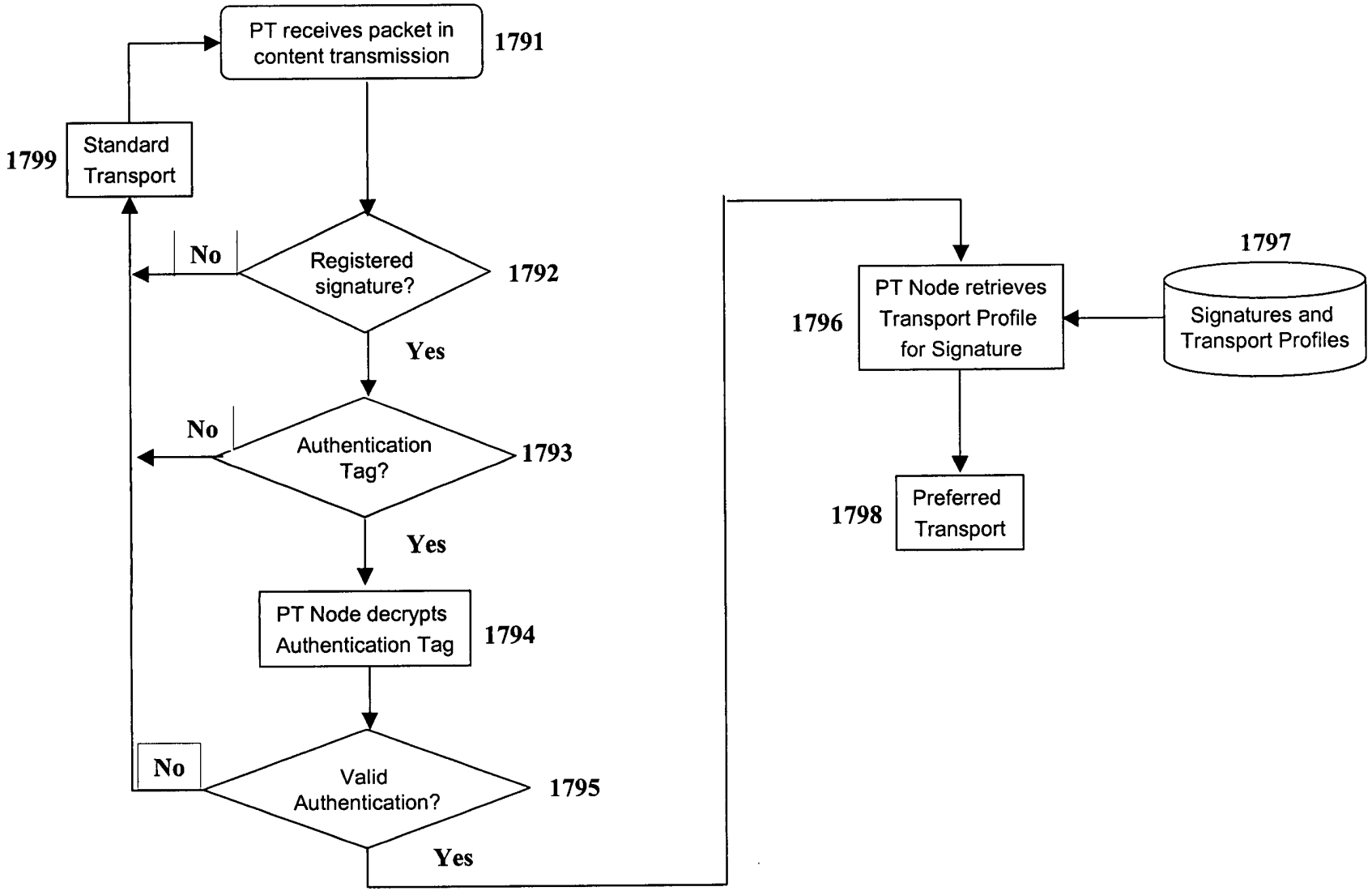

PT receives packet in content transmission
1791
Standard Transport
1799
No
Registered signature?
1792
Yes
No
Authentication Tag?
1793
Yes
PT Node decrypts Authentication Tag
1794
No
Valid Authentication?
1795
Yes
PT Node retrieves Transport Profile for Signature
1796
1797
Signatures and Transport Profiles
Preferred Transport
1798

Figure 22

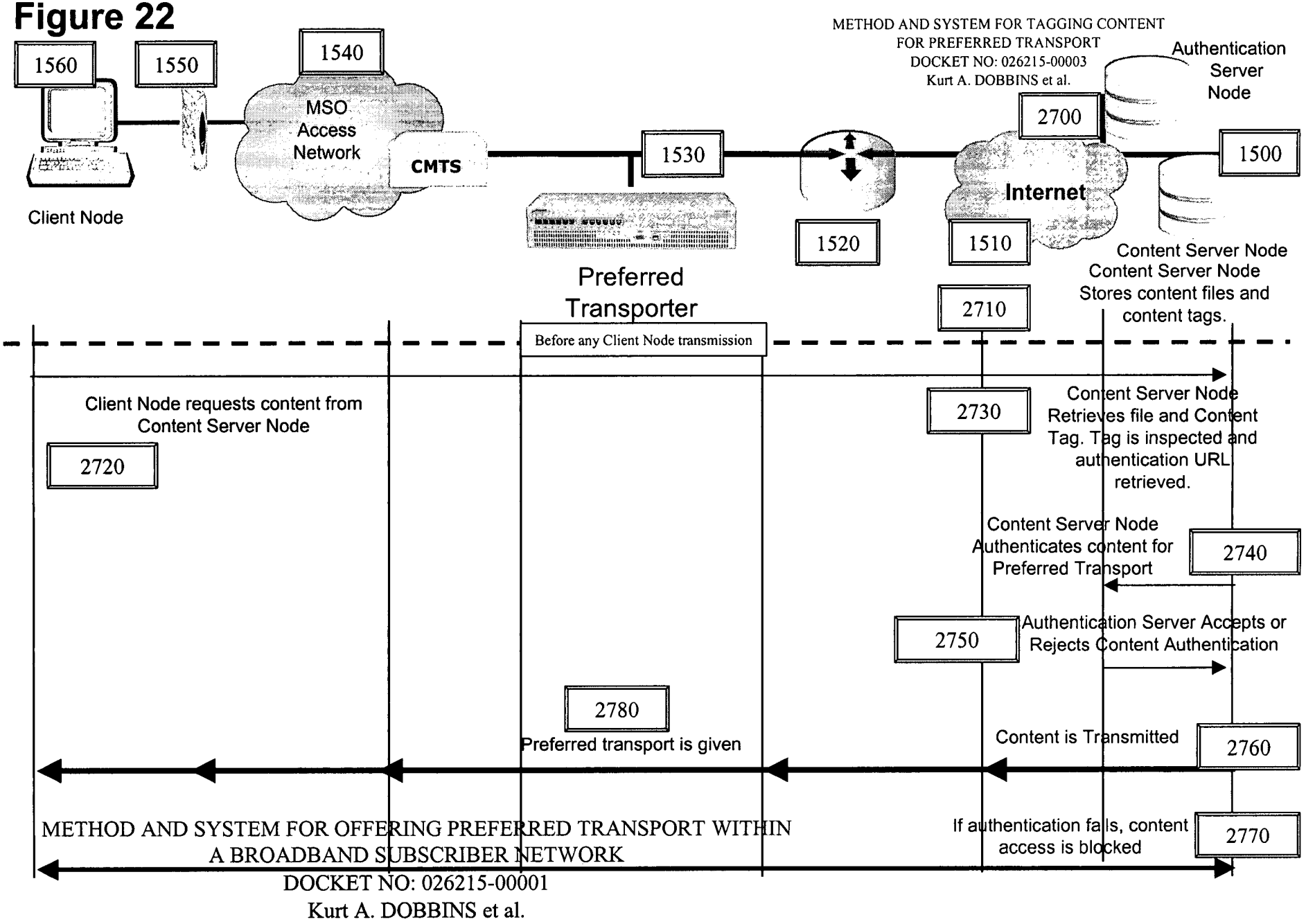

METHOD AND SYSTEM FOR TAGGING CONTENT
FOR PREFERRED TRANSPORT
DOCKET NO: 026215-00003
Kurt A. DOBBINS et al.
1560
1550
1540
MSO
Access
Network
CMTS
Client Node
1530
Preferred
Transporter
1520
2700
Authentication
Server
Node
1500
Internet
1510
Content Server Node
Content Server Node
Stores content files and
content tags.
2710
Before any Client Node transmission
Client Node requests content from
Content Server Node
2720
2730
Content Server Node
Retrieves file and Content
Tag. Tag is inspected and
authentication URL
retrieved.
Content Server Node
Authenticates content for
Preferred Transport
2740
2750
Authentication Server Accepts or
Rejects Content Authentication
2780
Preferred transport is given
Content is Transmitted
2760
If authentication fails, content
access is blocked
2770
METHOD AND SYSTEM FOR OFFERING PREFERRED TRANSPORT WITHIN
A BROADBAND SUBSCRIBER NETWORK
DOCKET NO: 026215-00001
Kurt A. DOBBINS et al.

Figure 22a

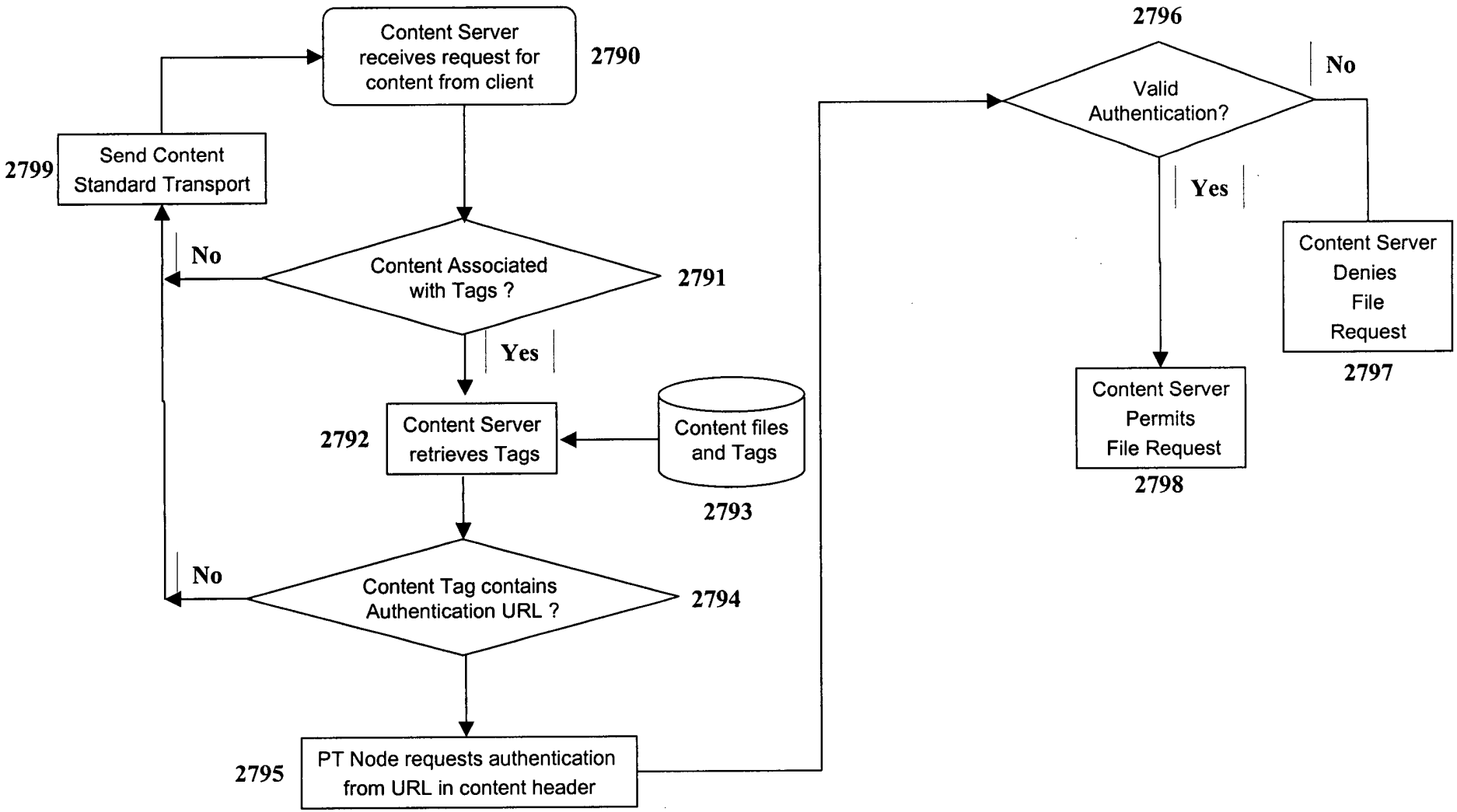
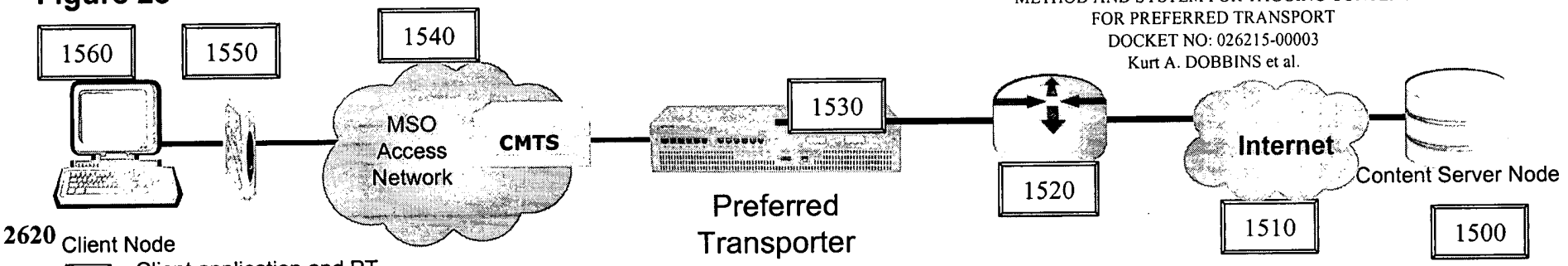

Content Server receives request for content from client
2790
Send Content Standard Transport
2799
No
Content Associated with Tags ?
2791
Yes
Content Server retrieves Tags
2792
Content files and Tags
2793
No
Content Tag contains Authentication URL ?
2794
PT Node requests authentication from URL in content header
2795
2796
Valid Authentication?
No
Yes
Content Server Denies File Request
2797
Content Server Permits File Request
2798

Figure 23



2620 Client Node

1 Client application and PT agree on signature, shared secret, and 1-way authentication aprioi.

2610

2 Content Server Node Stores content files

Before any Client Node transmission

2630 3 Client Node requests content from Content Server Node, inserting content tag into file request header

4 2640 PT Node receives file request with inserted tag. Tag is inspected and authenticated using 1-way authentication and shared secret.

2650

5 PT Node accepts or rejects based upon the result of the authentication.

6 2660 PT accepts

Preferred transport is given

6 PT rejects

No preferred transport is given or content access is blocked

Figure 23a

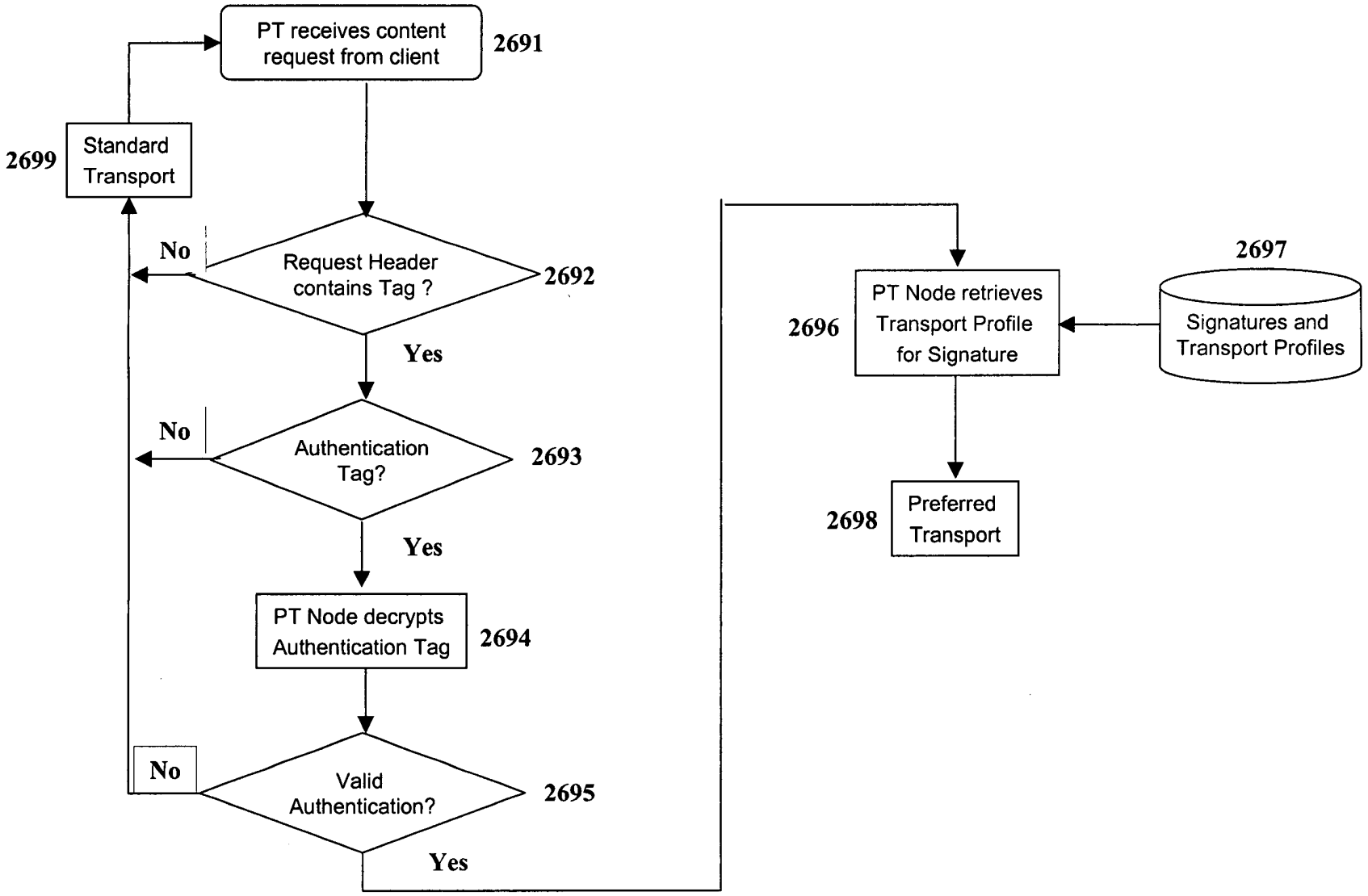

PT receives content request from client
2691
Standard Transport
2699
Request Header contains Tag ?
2692
No
Yes
Authentication Tag?
2693
No
Yes
PT Node decrypts Authentication Tag
2694
Valid Authentication?
2695
No
Yes
PT Node retrieves Transport Profile for Signature
2696
Signatures and Transport Profiles
2697
Preferred Transport
2698

Figure 24

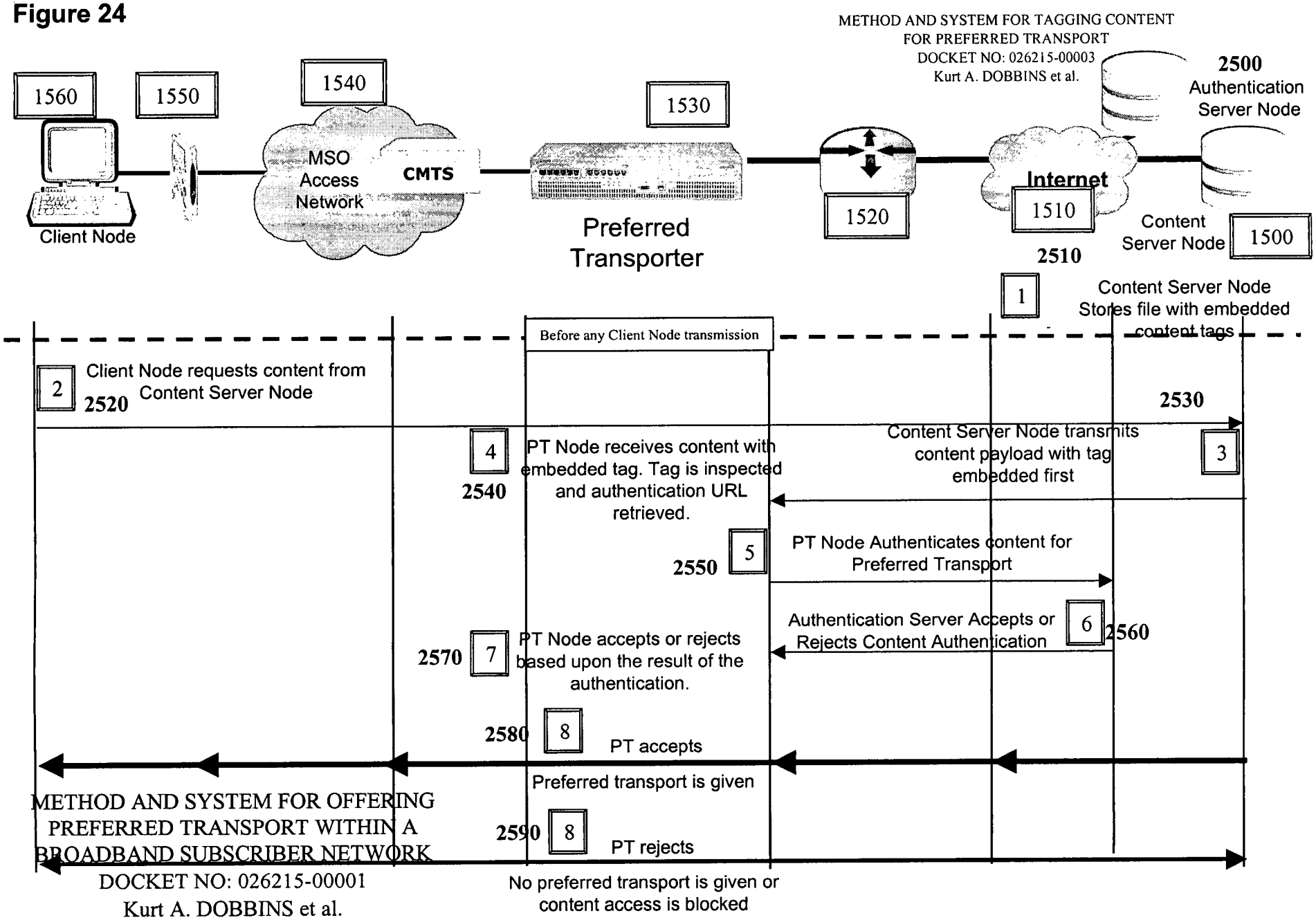

METHOD AND SYSTEM FOR TAGGING CONTENT FOR PREFERRED TRANSPORT
DOCKET NO: 026215-00003
Kurt A. DOBBINS et al.
1560
1550
1540
1530
1520
1510
2500
Authentication Server Node
Client Node
MSO Access Network
CMTS
Preferred Transporter
Internet
Content Server Node
1500
2510
1
Content Server Node Stores file with embedded content tags
Before any Client Node transmission
2
Client Node requests content from Content Server Node
2520
2530
3
Content Server Node transmits content payload with tag embedded first
4
2540
PT Node receives content with embedded tag. Tag is inspected and authentication URL retrieved.
5
2550
PT Node Authenticates content for Preferred Transport
6
2560
Authentication Server Accepts or Rejects Content Authentication
2570
7
PT Node accepts or rejects based upon the result of the authentication.
2580
8
PT accepts
Preferred transport is given
2590
8
PT rejects
No preferred transport is given or content access is blocked
METHOD AND SYSTEM FOR OFFERING PREFERRED TRANSPORT WITHIN A BROADBAND SUBSCRIBER NETWORK
DOCKET NO: 026215-00001
Kurt A. DOBBINS et al.

Figure 24a

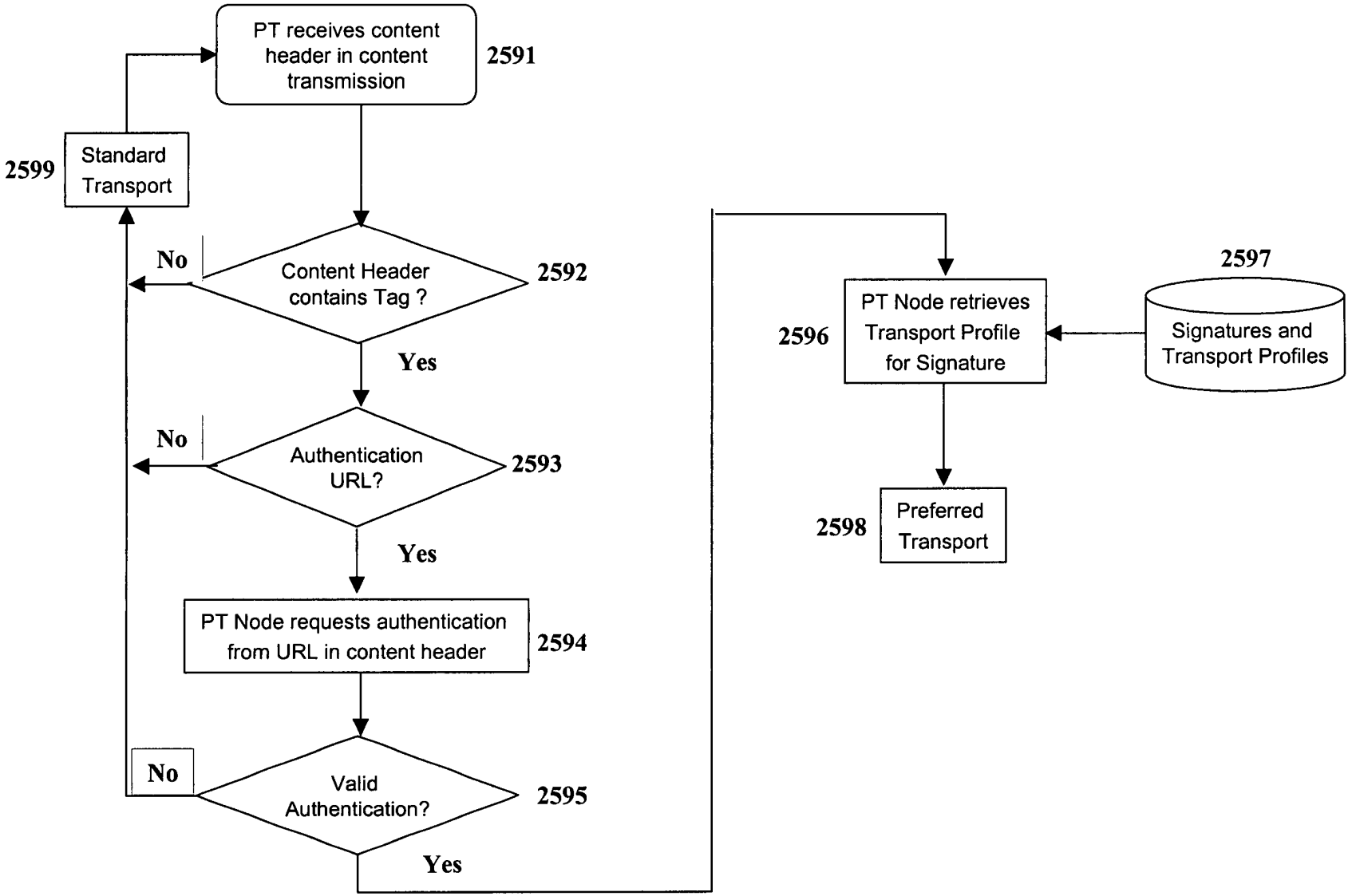

PT receives content header in content transmission
2591
Standard Transport
2599
No
Content Header contains Tag ?
2592
Yes
No
Authentication URL?
2593
Yes
PT Node requests authentication from URL in content header
2594
No
Valid Authentication?
2595
Yes
PT Node retrieves Transport Profile for Signature
2596
2597
Signatures and Transport Profiles
Preferred Transport
2598

Figure 25

- **Leverage OID Tree for Self-naming Tags**
  - Gives digital representation to textual names
  - Allows arbitrary hierarchy
  - Extensible with new content types
  - Packet encoding will use ASN.1 BER
- **Name Space Maintained by host**
  - Publish as Informational IETF MIB

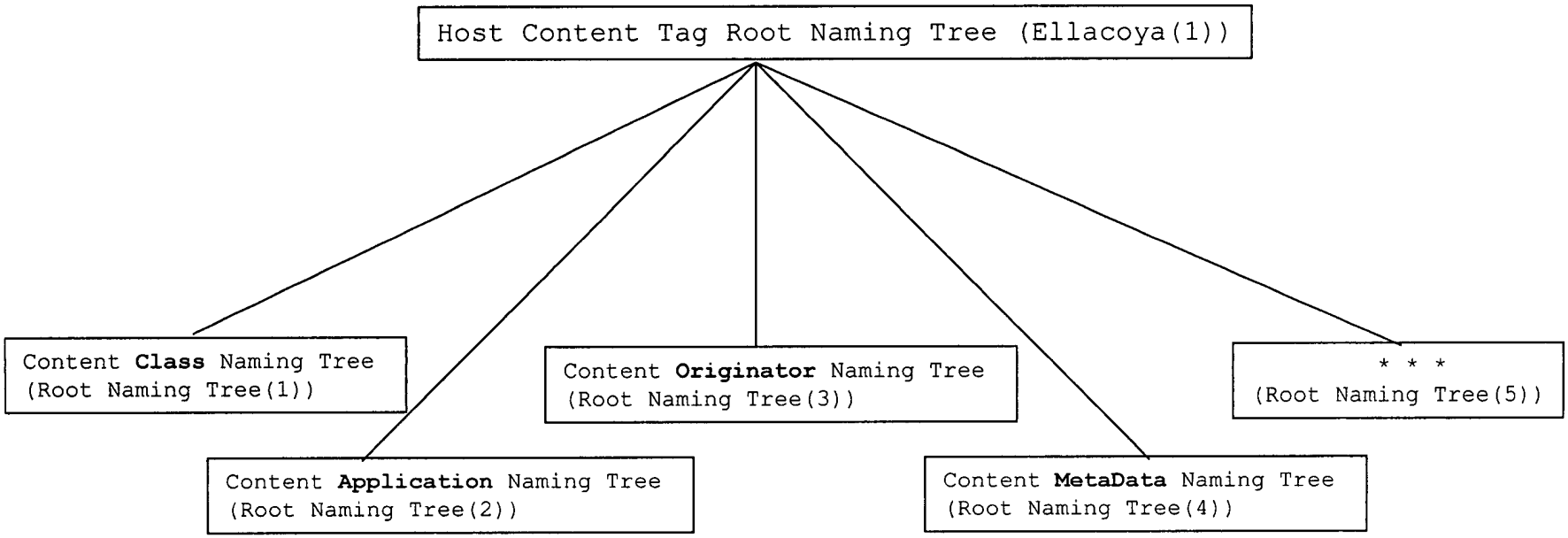


Figure 26

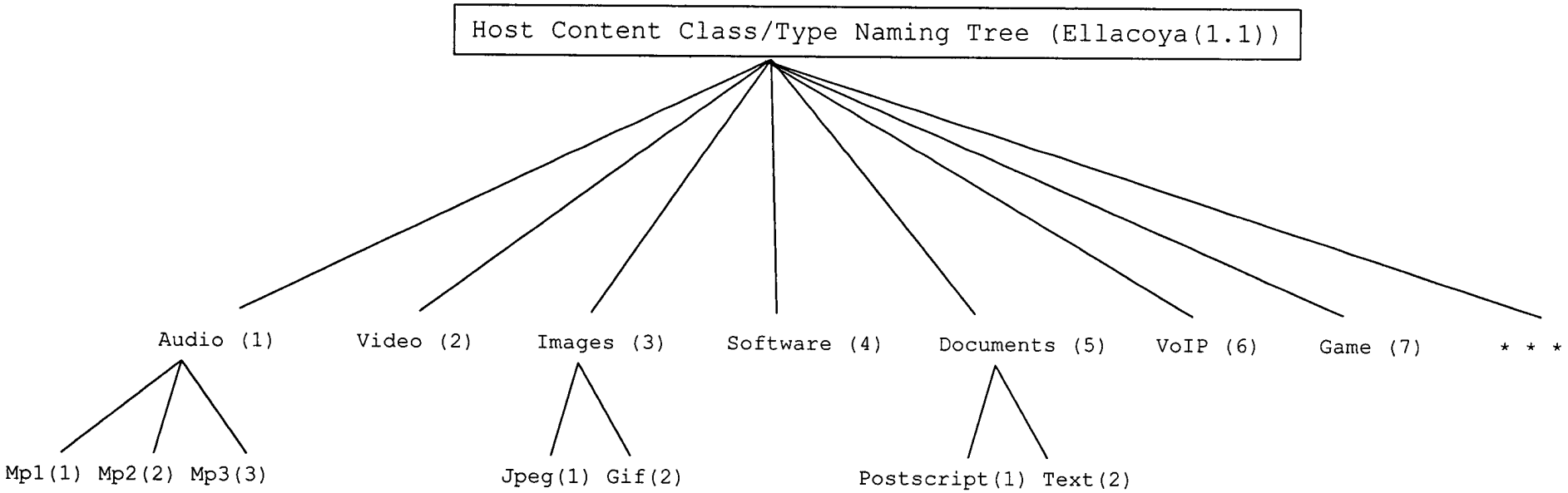

Host Content Class/Type Naming Tree (Ellacoya(1.1))
Audio (1)
Video (2)
Images (3)
Software (4)
Documents (5)
VoIP (6)
Game (7)
* * *
Mp1(1) Mp2(2) Mp3(3)
Jpeg(1) Gif(2)
Postscript(1) Text(2)

Figure 27

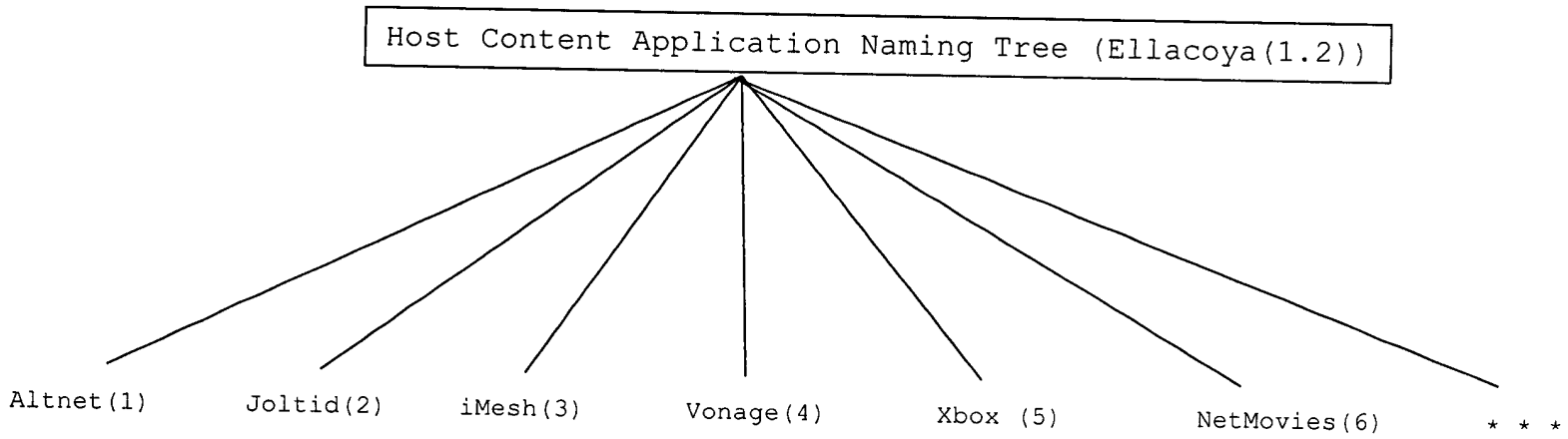
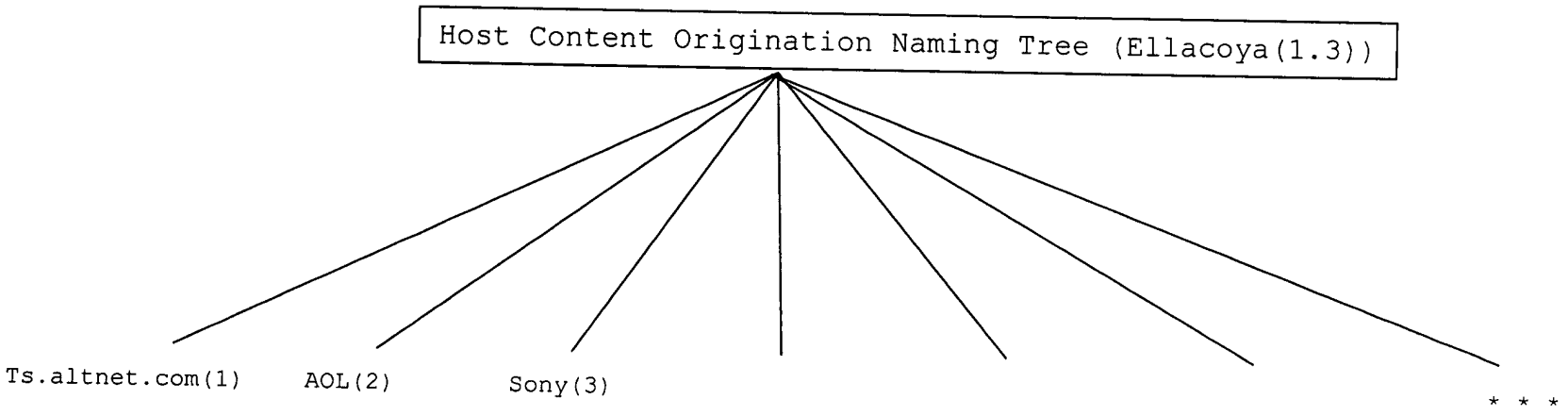

Host Content Application Naming Tree (Ellacoya(1.2))
Altnet(1)
Joltid(2)
iMesh(3)
Vonage(4)
Xbox (5)
NetMovies(6)
* * *

Figure 28


Host Content Origination Naming Tree (Ellacoya(1.3))
Ts.altnet.com(1)
AOL(2)
Sony(3)
* * *